Exhibit 18

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Gregory G. Raleigh	
U.S. Patent No.:	8,406,733	Attorney Docket No.: 39843-0164IP2
Issue Date:	March 26, 2013	
Appl. Serial No.:	13/461,141	
Filing Date:	May 1, 2012	
Title:	AUTOMATED DEVICE PROVISIONING AND ACTIVATION	

Mail Stop Patent Board
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR *INTER PARTES* REVIEW OF UNITED STATES PATENT NO. 8,406,733 PURSUANT TO 35 U.S.C. §§311–319, 37 C.F.R. §42

TABLE OF CONTENTS

APPENDIX OF CLAIMS

CLAIM 1	
1pre	***An end-user device comprising:***
1a	***a modem for enabling communication with a network system over a service control link provided by the network system over a wireless access network,***
1a1	***the service control link secured by an encryption protocol***
1a2	***and [the service control link is] configured to support control-plane communications between the network system and a service control device link agent on the end-user device;***
1b	***[the end-user device comprising:] a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus, each of the plurality of device agents identifiable by an associated device agent identifier; and***
1c	***[the end-user device comprising:] memory configured to store an encryption key,***
1c1	***the encryption key shared between the service control device link agent and a service control server link element of the network system;***
1d1	***wherein the service control device link agent is configured to: receive, over the service control link, an encrypted agent message from the service control server link element,***
1d2	***[wherein the service control device link agent is configured to:] using the encryption key, obtain a decrypted agent message,***
1d3	***the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of the plurality of device agents, the particular agent identifier identifying the particular device agent,***

1e	***the message content [being] from a particular server of a plurality of servers communicatively coupled to the service control server link element, and***
1f	***[wherein the service control device link agent is configured to:] based on the particular agent identifier, deliver the message content to the particular device agent over the agent communication bus.***
CLAIM 2	
2	***The end-user device recited in claim 1, wherein the particular server comprises a service usage history server, a policy management server, an access control integrity server, a network traffic analysis server, a beta test server, a service download control server, a billing event server, an activation server, a transaction server, an authentication server, or a content management server.***
CLAIM 3	
3	***The end-user device recited in claim 1, wherein the message content comprises information associated with a service usage.***
CLAIM 4	
4	***The end-user device recited in claim 3, wherein the information associated with the service usage comprises information about one or more of a service usage value, a projected service usage value, a service usage plan limit, a projected service usage overage, a projected service cost overage, a service plan period time duration, a service plan time remaining before end of period, and a service overage.***
CLAIM 5	
5	***The end-user device recited in claim 1, wherein the message content is based, at least in part, on a user preference.***
CLAIM 6	
6	***The end-user device recited in claim 1, wherein the message content comprises information associated with a roaming service usage or a roaming service cost.***

CLAIM 7	
7	***The end-user device recited in claim 1, wherein the message content comprises a service offer, an advertisement, or a transaction offer.***
CLAIM 8	
8	***The end-user device recited in claim 1, wherein the message content comprises information from a third party configured to provide control of a service or a billing for a service.***
CLAIM 9	
9	***The end-user device recited in claim 1, wherein the message content comprises an agent instruction, a setting value, an agent configuration, or a software update.***
CLAIM 10	
10	***The end-user device recited in claim 1, wherein the message content comprises software or a media file.***
CLAIM 11	
11	***The end-user device recited in claim 1, wherein the message content comprises information associated with a service policy.***
CLAIM 12	
12	***The end-user device recited in claim 1, wherein the message content comprises service usage accounting information.***
CLAIM 13	
13	***The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device message to the service control server link element over the service control link.***
CLAIM 14	
14	***The end-user device recited in claim 13, wherein the device message comprises a service usage report or an integrity report.***

CLAIM 15	
15	***The end-user device recited in claim 13, wherein the device message comprises a user response.***
CLAIM 16	
16	***The end-user device recited in claim 15, wherein the user response comprises an acknowledgment of a roaming cost or a roaming usage.***
CLAIM 17	
17	***The end-user device recited in claim 15, wherein the user response comprises an acknowledgment of a service usage, a service cost, or a service overage.***
CLAIM 19	
19	***The end-user device recited in claim 1, further comprising a user interface, and wherein the particular device agent is configured to assist in presenting a notification through the user interface, the notification based on the message content.***
CLAIM 20	
20a	***The end-user device recited in claim 19, wherein the particular device agent is further configured to: assist in obtaining a user response to the notification, and send a first message to the service control device link [agent], the first message comprising the user response,***
20b	***and the service control device link agent is further configured to: using the encryption key, generate an encrypted device message comprising the user response, and send the encrypted device message to a service control server link element over the service control link.***
CLAIM 21	
21	***The end-user device recited in claim 1, wherein the service control link supports asynchronous transmissions by the service control server link element.***

CLAIM 22	
22	***The end-user device recited in claim 1, wherein the service control link supports periodic transmissions by the service control server link element.***
CLAIM 23	
23	***The end-user device recited in claim 1, wherein the service control device link agent is further configured to send a device credential to the network system or receive the device credential from the network system during a service authorization sequence.***
CLAIM 24	
24	***The end-user device recited in claim 23, wherein the device credential comprises one or more of a phone number, an identification number, a security signature, a security credential, a subscriber identity module (SIM) identifier, a mobile equipment identifier (MEID), and a device identifier.***
CLAIM 26	
26	***The end-user device recited in claim 1, wherein the particular device agent comprises software.***
CLAIM 27	
27	***The end-user device recited in claim 1, wherein the encryption key is a first encryption key, and the service control device link agent is further configured to encrypt the message content using a second encryption key before delivering the message content to the particular agent, the second encryption key shared by the service control device link agent and the particular agent.***
CLAIM 28	
28	***The end-user device recited in claim 1, wherein the service control device link agent is further configured to trigger a device transmission to maintain the service control link when a time between transmissions would otherwise cause the service control link to terminate.***

CLAIM 29	
29	***The end-user device recited in claim 1, wherein the service control link is configured to support control-plane communications using an Internet protocol.***
CLAIM 30	
30Pre	***A method performed by an end-user device, the method comprising:***
30d1	***receiving, over a service control link, an encrypted agent message from a network element,***
30a1	***the service control link secured by an encryption protocol,***
30a2	***the service control link supporting control-plane communications between a service control device link agent on the end-user device and the network element;***
30d2	***using an encryption key…, obtaining a decrypted agent message***
30c	***[the] encryption key shared between the service control device link agent and the network element***
30d3	***the decrypted agent message comprising a particular agent identifier and message content for delivery to a particular device agent of a plurality of device agents on the end-user device,***
30b	***each of the plurality of device agents identifiable by an associated device agent identifier and communicatively coupled to the service control device link agent through an agent communication bus,***
30d4	***the particular agent identifier identifying the particular device agent,***
30e	***the message content [being] from a particular server of a plurality of servers communicatively coupled to the network element; and***
30f	***delivering the message content to the particular device agent over the agent communication bus based on the particular agent identifier.***

EXHIBITS

EX-1001	U.S. Patent No. 8,406,733 to Raleigh (“the ’733 Patent”)
EX-1002	Excerpts from the Prosecution History of the ’733 Patent (“the Prosecution History”)
EX-1003	Declaration and Curriculum Vitae of Dr. Patrick Traynor
EX-1004	**RESERVED**
EX-1005	U.S. Pat. No. 8,195,961B2 (“Ogawa”)
EX-1006	PCT Pat. App. Pub. No 2006/077283A1 (“Houghton”)
EX-1007	EP Pat. App. Pub. No. 1,909,463A1 (“Hwang”)
EX-1008	PCT Pat. App. Pub. No. WO 2008/048075A1 (“Lee”)
EX-1009	U.S. Pat. No. 7,975,147B1 (“Qumei”)
EX-1010	U.S. Pat. No. 9,032,192B2 (“Frank”)
EX-1011	**RESERVED**
EX-1012	**RESERVED**
EX-1013	The Secure Sockets Layer (“SSL”) Protocol, V. 3.0, available at *https://web.archive.org/web/19970614041044/http://home.netscape.com/eng/ssl3/ssl-toc.html* and *https://web.archive.org/web/19970617034012/http://home.netscape.com/eng/ssl3/3-SPEC.HTM#1*
EX-1014	The Transport Layer Security (“TLS”) Protocol, V. 1.1, available at *https://www.ietf.org/rfc/rfc4346.txt*
EX-1015	US. Pat. App. Pub. No. 2003/0096625 (“Mi-Su Lee”)
EX-1016	US Pat. No. 7,844,915 B2 (“Platzer”)
EX-1017	US Pat. No. US 8,370,818 (“Osminer”)

EX-1018	**RESERVED**
EX-1019	**RESERVED**
EX-1020	USPTO Binding Interim Guidance Addressing PTAB's Approach to Discretionary Denials, June 21, 2022, available at *https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf*
EX-1021	Plaintiff Headwater Research LLC's Disclosure of Asserted Claims And Infringement Contentions, *Headwater Research LLC v. Samsung Electronics Co.*, 6:23-cv-00103-JRG-RSP (WDTX)
EX-1022	Docket Control Order , 2:23-CV-00103-JRG-RSP, [63] December 1, 2023
EX-1023	Samsung Stipulation letter regarding IPR grounds in District Court Litigation
EX-1024	**RESERVED**
EX-1025	**RESERVED**
EX-1026	U.S. Patent No. 7,509,487 to Lu et al. ("Lu")
EX-1027	U.S. Patent Pub. No. 2005/0207379 to Shen et al. ("Shen")
EX-1028	*Transporting data between wireless applications using a messaging system—MMS*, Miraj E Mostafa, Wireless Communications and Mobile Computing (2007) ("Mostafa")
EX-1029	Dictionary of Computer Science, Engineering, and Technology, CRC Press LLC, 2001
EX-1030	**RESERVED**

EX-1031	U.S. Patent No. 8,010,669 to Sathish
EX-1032	**RESERVED**
EX-1033	U.S. Patent No. 6,101,485 to Fortenberry
EX-1034	U.S. Patent Pub. No. 2009/0037270 to Patro
EX-1035	**RESERVED**
EX-1036	**RESERVED**
EX-1037	**RESERVED**
EX-1038	Plaintiff Headwater Research LLC's Amended Infringement Contentions, *Headwater Research LLC v. Samsung Electronics Co.*, 6:23-cv-00103-JRG-RSP (WDTX)
EX-1039	**RESERVED**
EX-1040	**RESERVED**

I. IPR REQUIREMENTS

A. Grounds for Standing

Petitioners Samsung Electronics Co., Ltd. and Google LLC certify that the ’733 Patent is available for IPR and that Petitioners are not barred or estopped from this review. 37 C.F.R. §42.104(a).

B. Challenge and Relief Requested

Petitioners request IPR of the Challenged Claims on the grounds below. EX-1003, ¶¶1-47, 239-424.

Ground	Challenged Claim(s)	35 U.S.C. §103
2	1, 2, 5, 7-10, 13-15, 19-22, 26-30	Houghton-Ogawa
3	3-4, 6, 11-12, 16-18, 23-24	Houghton-Ogawa-Hwang

Reference	Filing Date	Publication Date	Prior Art basis
Ogawa	5/19/2008	10/1/2009	102(a)/102(e)
Houghton	1/20/2005	7/27/2006	102(b)
Hwang	10/16/2006	4/9/2008	102(a)/102(e)

C. Claim Construction

Claim terms are construed herein using the standard used in civil actions under 35 U.S.C. §282(b), in accordance with the ordinary and customary meaning as understood by a POSITA and the patent’s prosecution history. 37 C.F.R.

§42.100(b). The Board need only construe terms to the extent necessary "to resolve [a] controversy." *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017). Petitioners are not conceding that each Challenged Claim satisfies all statutory requirements, nor waiving arguments that can only be raised in district court.

D. Level of Ordinary Skill in the Art

A person of ordinary skill in the art ("POSITA") relating to the subject matter of the '733 Patent as of January 28, 2009 ("Critical Date"), would have had (1) at least a bachelor's degree in computer science, electrical engineering, or a related field, and (2) 3-5 years of experience in services and application implementation in communication networks. EX-1003, ¶¶21-22, 1-15. Additional graduate education could substitute for professional experience, and vice versa. *Id.*

II. THE '733 PATENT

A. Brief Description

The '733 Patent is directed to "devices" "receiving control-plane communications from a network element over a secure service control link." EX-1001, Abstract. Control-plane communications include communications sent over a network "involving supervision" and "control" of "service[s]" being delivered to a device. EX-1001, 37:34-46, 68:19-28; EX-1003, ¶42.

FIG. 16 (below) shows ***service control link 1653*** between service controller 122's ***service control server link 1638*** and device 100's ***service control device link***

1691. *Id.*; EX-1003, ¶43. Service control link 1653 is a "control plane communication link" providing "communications between the [device's] service processor 115 and the service controller 122." EX-1001, 68:28-37.

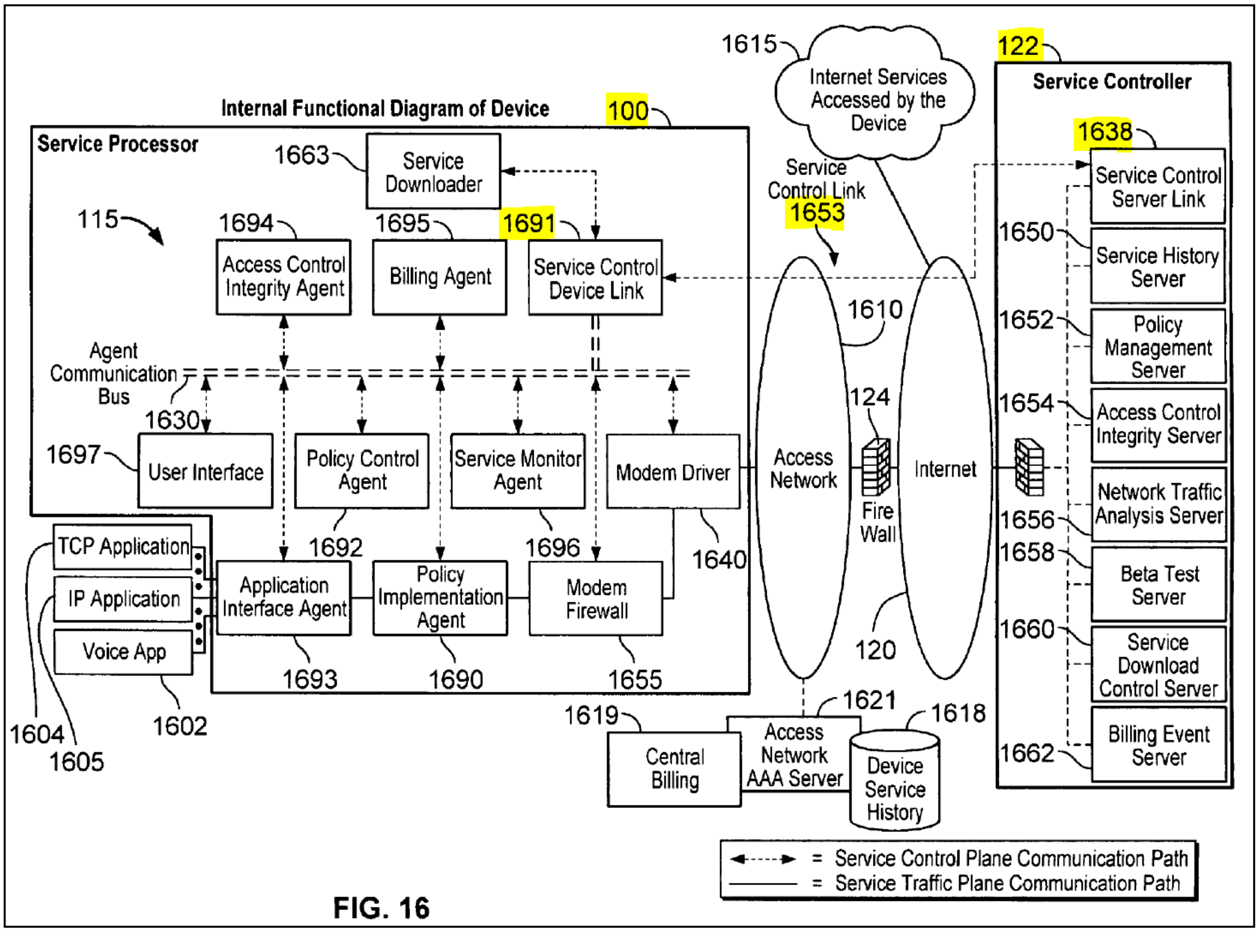


FIG. 16

EX-1001, FIG. 16 (annotated)

The specification describes multiple "layers of encryption in the service control link," with one layer "implemented in the transport services stack." EX-1001, 87:58-63. For "secure control plane communication[s]" received by a device over link 1653, service control device link 1691 "decode[s]" (*e.g.*, "decrypts"), unpacks, and routes the communication "to the appropriate agent" on the device. *Id.*, 87:49-58, 89:21-33, 90:19-53; EX-1003, ¶¶44-45.

B. Prosecution History

The '733 Patent issued after one Office Action that included only §112 rejections. EX-1002, 97-101. The Examiner did not consider Houghton, Ogawa, or Hwang. EX-1003, ¶¶46-47.

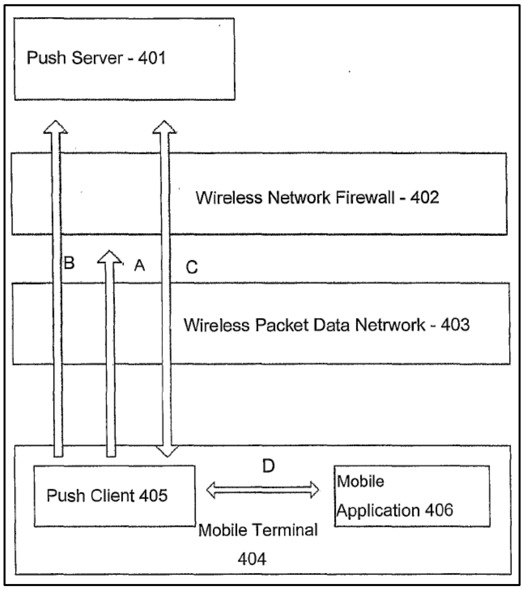
III. THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 2: Claims 1, 2, 5, 7-10, 13-15, 19-22, and 26-30 Are Obvious Over Houghton and Ogawa

1. Houghton

Houghton discloses pushing commands from a server to a mobile terminal (which Houghton also calls a "client device") to "initiate control of… applications on [the] terminal." EX-1006, 10-11[1], 14-15; EX-1003, ¶239. An exemplary embodiment is shown in Houghton FIG. 4:

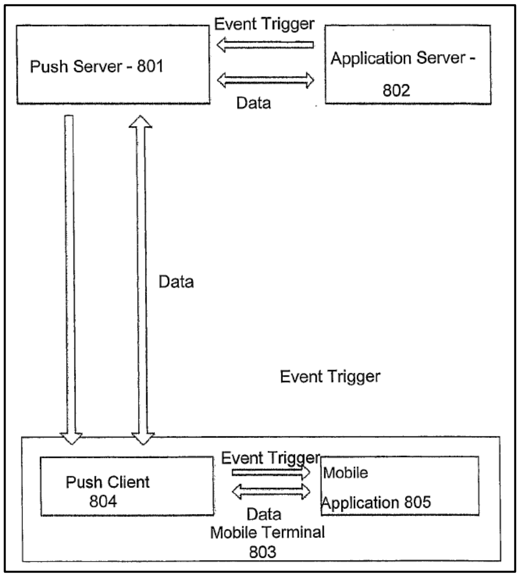
[1] References to Houghton (EX-1006) are to page numbers printed on the document rather than to page numbers stamped on the exhibit.



EX-1006, Figure 4

P***ush client 405*** on ***mobile terminal 404*** and ***push server 401*** send and receive messages through ***data connection C***. *Id*., 20. Push messages (from a push server) include "application-specific" information "specifying which mobile application 406" on mobile terminal 404 is the push message's target. *Id*., 21; EX-1003, ¶240.

Data connection C is used to "establish[]" a "connection between [a separate] application server 802" and the mobile application on the mobile terminal, as shown below. *Id*., 23; EX-1003, ¶241.



EX-1006, Figure 8

In Houghton, a "'COMMAND PUSH' procedure" is used, "wherein the push server… is triggered by a trigger event… from an application server… to push an application command message to the push client… and thereby initiate a mobile terminal client trigger event in a mobile application." EX-1006, 23; EX-1003, ¶242 (discussing EX-1006, 21-22).

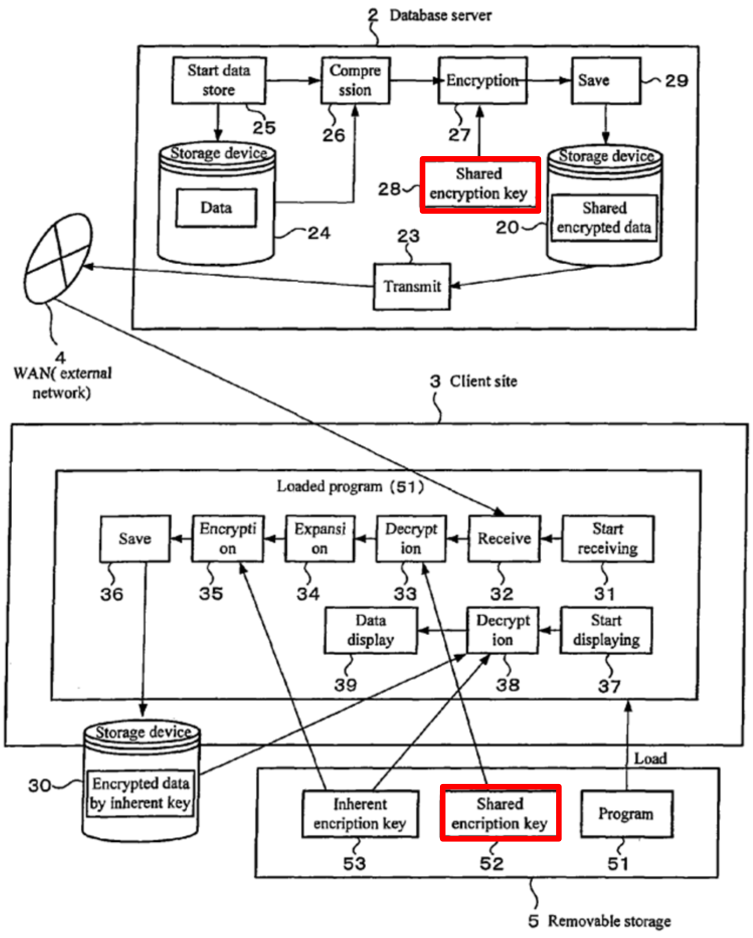
Herein, components of Houghton's system in which the mobile terminal uses data connection C to exchange messages with an application server through a push server are sometimes referred to using reference numbers from both Figures 4 and 8 (*e.g.*, mobile terminal 404/803, push client 405/804). EX-1003, ¶243.

Houghton discloses using a "connection-oriented protocol such as TCP/IP, SSL [Secure Socket Layer], HTTP or HTTPS" to facilitate a secure communication link between the push server and mobile terminal. EX-1006, 20; EX-1003,

¶244. Houghton also discloses "exchanging security keys" between server and client. EX-1006, 29.

2. Ogawa

Ogawa discloses a "data encryption system" for securing communications between database server 2 and client site 3 through network 4, shown below. EX-1005, 3:18-21, 9:15-20, FIG. 7; *see also id.*, FIG. 1, 3:44-54; EX-1003, ¶¶54-56 (explaining that FIG. 7 illustrates a client-server system that performs functions described for FIG. 1).



EX-1005, FIG. 7 (annotated).

In Ogawa, "SSL (Secure Socket Layer), is utilized to prevent some security risks presented during the exchange of data between network terminals." EX-1005, 3:61-4:4, 9:16-34. EX-1003, ¶57.

Ogawa teaches ***further*** encrypting data using a "shared encryption key" distributed to (and used by) the client and server. EX-1003 ¶58 (citing EX-1005, 6:42-47, 7:11-21, 9:16-20). The key is used to (1) encrypt data that is transmitted (as encrypted data) to the client, and (2) decrypt received encrypted data at the client. EX-1005, 9:21-34, 5:60-65. Decryption is conducted by a "decryption unit" on the client. EX-1005, 5:59-6:9; EX-1003, ¶¶59-60.

3. Houghton-Ogawa Combination

(a) Implementing Houghton's Mobile Terminal with a Modem

Houghton's mobile terminal is "located in [a] wireless network," and software on the terminal communicates with servers "over a data network 403," *e.g.*, a wireless network that can transmit "Internet Protocol (IP) packets." EX-1006, 11, 17. Houghton's terminal is also "equipped" to establish "a connection" to a "broadband network access point" via "a wireless communication network," *e.g.*, Bluetooth, "Wi-Fi, Wi-Max or other personal area, local area, metropolitan, or large area network." *Id.,* 13-14.

While Houghton does not disclose details regarding how its mobile terminal facilitates communications over the above-described wireless networks, using a modem for enabling communications with such wireless networks was well-known before the Critical Date. EX-1003, ¶¶245-246 (citing EX-1008, ¶¶27-28, 44, 46, 50-52, FIGS. 1, 4). Using a modem to enable a user device to communicate over Houghton's wireless networks would have been a conventional and obvious way to implement what Houghton describes, and involves utilizing familiar, known components to achieve a predictable result of facilitating Houghton's communications. *KSR Int'l v. Teleflex*, 550 U.S. 398, 416 (2007); EX-1003, ¶247 (citing EX-1008, FIG. 4, ¶¶[22-23]). A POSITA would also have reasonably expected success implementing Houghton's device with a modem because modems were a well-known, conventional way of achieving the wireless network communications Houghton describes. EX-1003, ¶247.

(b) Applying Ogawa's Symmetric Encryption Techniques

Houghton discloses using SSL for securing communication links between the push server 401 and push client 405. EX-1006, 20, 18; EX-1003, ¶248.

Houghton also describes "exchanging security keys" between the server and the client (EX-1006, 29) but does not provide details regarding this key exchange. It was well-known for data in messages transmitted between a server and a client to be encrypted using symmetric encryption, with a key that is shared between the server and the mobile terminal and stored in their respective memories. EX-1003, ¶248 (citing, *e.g.*, EX-1027, [0054]-[0060]; EX-1005, 3:44-53, 9:16-34; EX-1009, 3:25-27, 8:1-15). Ogawa discloses details regarding how to implement such symmetric encryption of messages sent between a server and a client. EX-1003, ¶248 (EX-1005, 3:44-53, 9:16-34).

A POSITA had multiple reasons to implement Ogawa's symmetric data encryption techniques with Houghton ("Houghton-Ogawa Message Encryption").

First, implementing the data encryption taught in Ogawa to Houghton's communicated messages would have achieved a "protected" push messaging system that beneficially "protect[s] the mobile terminals from hostile or unwanted contact common on the public Internet" (utilizing "exchang[ed] security keys"), consistent with Houghton's teachings. EX-1006, 17, 29; EX-1003, ¶¶249-250.

Second, both references describe systems in the field of client-server communications, and Ogawa explains how an additional layer of symmetric encryption can be implemented for securing communications in server-client networked environments which already utilize, *e.g.*, SSL, as described in Houghton. EX-1005, 3:44-53, 3:60-4:4, 4:48-57, 5:59-65, 6:64-7:21, 9:16-34; EX-1003, ¶251 (noting that Ogawa's technique was well-known and corroborated by, *e.g.*, EX-1009, 3:25-27, 8:1-5). Given Ogawa's express teachings, the well-known use of symmetric data encryption in SSL-protected client-server environments like Houghton's, and the consistency between Ogawa's teachings and Houghton's teachings of security key exchange, a POSITA would have been motivated to implement Ogawa's encryption teachings of using a shared encryption key to encrypt Houghton's server-client communications. EX-1003, ¶251.

Third, implementing the techniques described in Ogawa to Houghton's SSL-protected system would have beneficially enhanced security of data communications occurring over Houghton's network. EX-1003, ¶252. Ogawa teaches using two forms of encryption for client-server communications instead of one—data encryption to encrypt data sent over a secure communication channel (*e.g.*, SSL-based connection)—which would have motivated implementing the same dual encryption techniques within Houghton's system. *Id*.

Fourth, implementing Ogawa's data encryption into Houghton's system would have been nothing more than implementing known methods/techniques (symmetric encryption using a shared key as taught in Ogawa) to known systems/devices (push server and mobile terminals with push clients, per Houghton) to achieve predictable results (data encryption over messages transmitted on a secure SSL, as Houghton contemplates). EX-1003, ¶253.

Implementing Ogawa's encryption techniques in Houghton's system would have been predictable and straightforward, and a POSITA would have had a reasonable expectation of success in doing so, given (1) the similar client-server communication architectures taught by both references, (2) Houghton's teaching of key exchange for message encryption, and (3) Ogawa's (and the above-described corroborating references') provision of an exemplary implementation of such encryption using a symmetric/shared encryption key within an SSL-protected network environment. EX-1003, ¶254.

(c) Ogawa's Decryption and Encryption Units

Ogawa teaches a "decryption unit" for decrypting received encrypted data as part of its symmetric encryption system. EX-1005, 5:59-6:9. A POSITA would have had reason to implement Ogawa's decryption unit within Houghton's push client to facilitate decryption of encrypted data received from the push server because Houghton's push client is responsible for receiving messages and distributing them to the correct mobile applications on the mobile terminal. EX-1003, ¶255. Such an implementation would have beneficially allowed Houghton's push client to decrypt an encrypted message from the push server and obtain received information identifying the destination application to which the message should be routed. *Id*.

Ogawa also teaches an encryption unit for encrypting (or "re-encrypt[ing]") data before transmitting it to another entity on the network (*e.g.*, a server) or another part of the device, *e.g.*, storage. EX-1005, 5:59-6:9; EX-1003, ¶256. As with the decryption unit, a POSITA would have had reason to implement the encryption unit as part of the Houghton's push client, because enabling secure transmission of data to other components residing on the device such a storage unit, per Ogawa, was a desirable feature that would have helped prevent, *e.g.*, data theft. EX-1003, ¶256.

A POSITA would have reasonably expected success in implementing Ogawa's encrypt and decrypt units within Houghton's push client, because the prior art elements of this system would each perform functions they performed prior to the combination—Houghton's system would continue to provide the push communications between push clients and push server using secure data connection C, and Ogawa's decrypt and encrypt units (implemented within the push client) would continue to facilitate encryption/decryption to secure the data received from the push server. EX-1003, ¶257. Such a combination would have been well within a POSITA's capability to implement. *Id.*

(d) Storing Ogawa's Shared Encryption Key

Houghton discloses that its mobile terminal is "capable of receiving and ***storing*** variables which configure behavior of the client," and discloses "***stored***"[2] "username, password, and security certificates." EX-1006, 22-23. A POSITA thus understood that Houghton's mobile terminal has memory. EX-1003, ¶258. Alternatively, such an implementation would have been a conventional and obvious

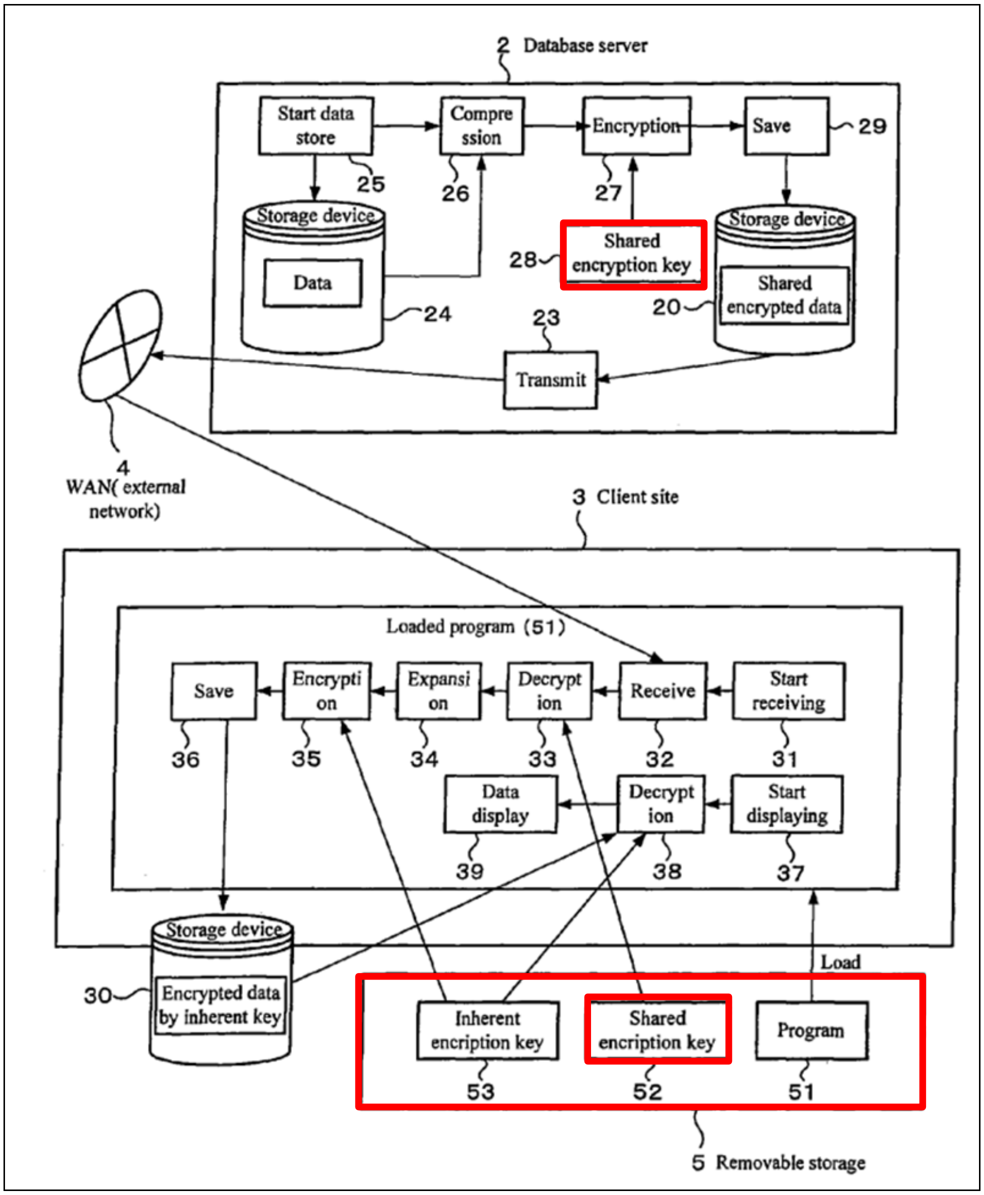
[2] Emphasis is added throughout unless otherwise indicated.

way to implement the "storing" that Houghton describes, and involves utilizing familiar, known components (memory) to achieve a predictable result of storing data on a mobile terminal. *Id.*

Ogawa teaches the well-known technique of ensuring that each device/entity in a network environment that encrypts or decrypts communications using symmetric encryption ***stores*** the encryption key in memory connected to it. EX-1005, 3:18-34, 4:48-57, 5:59-65, 6:64-7:21, FIGS. 1, 7; EX-1003, ¶259 (citing EX-1009, 8:1-5, 3:25-27; EX-1006, 29, claim 3). For symmetric encryption, there were a limited number of ways to ensure the same key was used by encrypting/decrypting devices, including (1) storing the same key by each encrypting/decrypting device in persistent memory, and (2) generating the same key at each device prior to performing the encrypting/decrypting operation, and storage of that key temporarily during the operation. EX-1003, ¶259. In both ways, the key was stored during the encryption/decryption. *Id.*

A POSITA would have had multiple reasons to store Ogawa's encryption key in the memory of Houghton's mobile terminal to facilitate decryption of encrypted messages received from Houghton's push server.

First, an implementation in which the encryption key was stored in the Houghton mobile terminal's memory would have been a way to implement Ogawa's symmetric encryption teachings, which discloses storing the shared encryption key in removable storage 5 that is connected to client site 3 and functions as a memory for client site 3, so that the key can be retrieved and used when needed to decrypt a message. EX-1005, 3:61-4:7, 5:41-47, 9:21-34, FIG. 7; EX-1003, ¶¶260-261.



EX-1005, FIG. 7 (annotated)

Storing Ogawa's encryption key in the memory of Houghton's mobile terminal (*i.e.*, the client site, in Ogawa's terminology) would have beneficially enabled the Houghton's push client (modified to include Ogawa's decryption and encryption units, as discussed above) to access the key and perform the decryption/encryption described in Ogawa. EX-1003, ¶262.

Second, such an implementation would have been nothing more than implementing a known method (storage of a symmetric/shared key in memory as taught by Ogawa and background references) to known systems (Houghton's push system, including a mobile terminal with memory) to achieve a predictable result of enabling Ogawa's symmetric encryption/decryption in Houghton's push system. EX-1003, ¶263.

Third, storing the shared key on a memory within Houghton's mobile terminal would have been an obvious, readily-implementable design choice that a POSITA would have known would facilitate storing Ogawa's encryption key within a location accessible to the mobile terminal, as required for symmetric encryption. EX-1003, ¶¶264-267. That this design was well-known to POSITAs is corroborated by references like Qumei, which describes storing the "enciphering key" in an end-user device (*e.g.*, a mobile handset). EX-1009, 3:25-27; EX-1003, ¶264; *see also id.* (citing EX-1005, 5:42-58).

Storing the encryption key in the Houghton terminal's memory and enabling it to be retrieved from memory when needed would have been well within a POSITA's skill to implement, and a POSITA would have reasonably expected success in doing so, because this would have involved using components to perform the functions they performed prior to the combination. EX-1003, ¶268.

(e) Houghton-Ogawa

"Houghton-Ogawa" refers to the above-discussed encrypted push system that a POSITA would have been led to form based on Houghton and Ogawa.

Houghton-Ogawa implements Houghton's mobile terminal (configured to use the push system as described in Houghton) with a modem for wireless network communications. *Supra* §III.A.3(a).

Houghton-Ogawa also implements Houghton's push server and mobile terminal so that the communication link between them is secured using SSL and transmitted messages are further encrypted using symmetric Houghton-Ogawa Message Encryption. *Supra* §III.A.3(b).

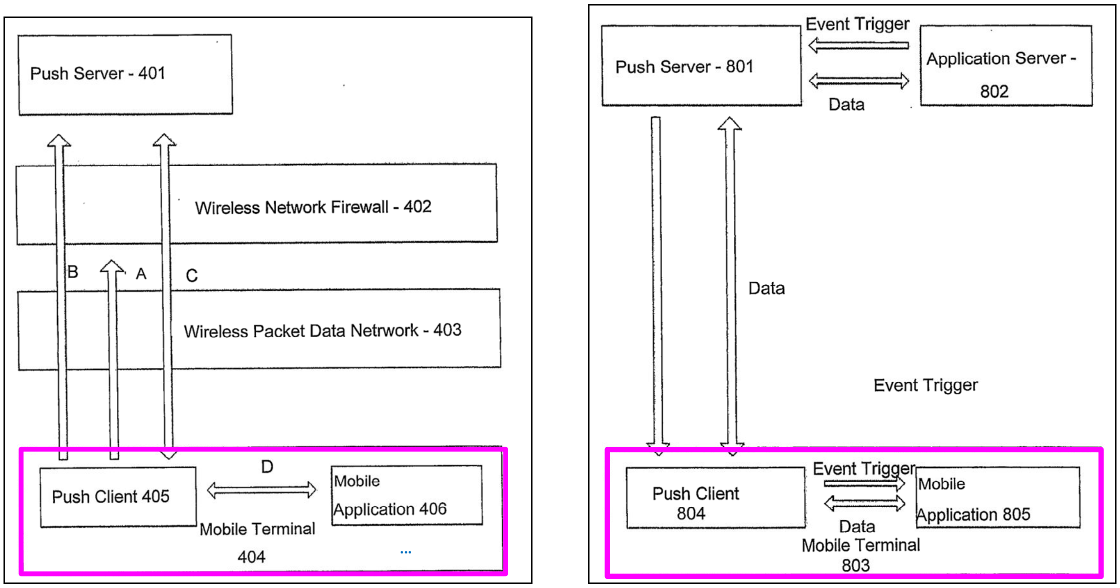
In Houghton-Ogawa, Ogawa's encrypt and decrypt units are implemented within the push client in Houghton's mobile terminal (*supra* §III.A.3(c)), and a common key is distributed to (and stored in the respective memories of) Houghton's mobile terminal and push server (*supra* §III.A.3(d)). EX-1003, ¶¶269-272.

4. Claims

(a) Claims 1 and 30

[1pre]/[30pre][3]

The ’733 specification does not define any requirements for an “end-user device” (*see* EX-1001, 8:3-15, 8:60-9:15), using the term to include a “networked” device that has “services [for a user] delivered” to it. EX-1001, 5:65-6:28, 6:49-56; EX-1003, ¶273. If the preambles are limiting, a POSITA understood Houghton-Ogawa’s mobile terminal 404/803 is an “end-user device,” because it operates “under supervision” of a user and is a networked device to which services for the user are delivered. *See* EX-1006, 17, 12, 22; EX-1003, ¶273.



EX-1006, FIG. 4 (annotated, left); FIG. 8 (annotated, right)

[3] Limitations herein are identified using reference labels from the Claim Appendix.

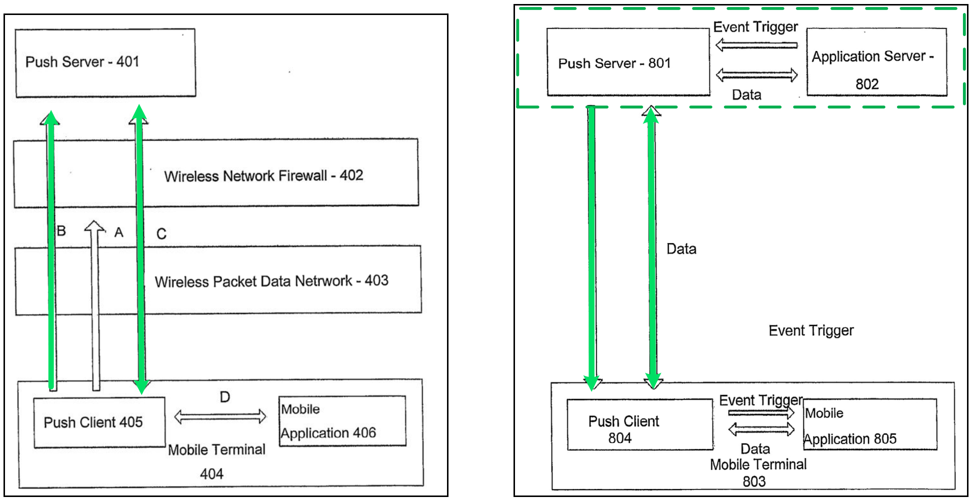
As described below, Houghton-Ogawa's mobile terminal 404/803 performs claim 30's method. EX-1003, ¶274.

[1a]

[1a] requires "a ***modem*** for enabling communication" taking place "over a wireless access network." A POSITA understood Houghton-Ogawa's modem for connecting to a "wireless communication network such as… Wi-Fi" that provides access to a "broadband network" (*supra* §III.A.3(a)) is a "modem for enabling communication" occurring "over a wireless access network" (as claimed)—just like the '733 Patent's "Wi-Fi" modem that provides access to "DSL" and "cable" networks. EX-1001, 25:29-45, 27:38-44, 29:52-67, 33:59-65; EX-1003, ¶275.

[1a] also requires that the modem enable communication "with a ***network system*** over a service control link." The '733 specification never describes a "***network system***" in the context of a "service control link." EX-1003, ¶276. Based on the '733 specification's disclosures regarding communications with a "network" over a "service control link," a POSITA understood that one or more servers performing one or more server functions would meet the claimed "network system." EX-1003, ¶276 (citing EX-1001, 16:13-26, 17:8-11, 68:20-37, FIGs. 16-20).

In Houghton-Ogawa, mobile terminal 404/803's modem enables it to communicate with push server 401/801 and application server 802. EX-1006, 23; EX-1003, ¶277.



EX-1006, FIG. 4 (annotated, left); FIG. 8 (annotated, right)

A POSITA understood that push server 401/801 and application server 802 (outlined with dashed-lines above) are a "network system," because (1) the specification only describes a "service control link" as connecting a device to a "network" that comprises one or more servers performing one or more server functions and thus the claimed "network system" encompasses at least that, and (2) the push server and application server perform server functions. EX-1003, ¶278 (citing EX-1001, 16:13-26, FIGs. 16-20; EX-1006, 16-17, 23; *see also* discussion *infra* regarding [1e]).

Regarding "***service control link***," the '733 specification does not set forth any requirements but says it "can provide [a] control plane communication link" used for "***controlling***" some aspect of a "service" (*e.g.*, "data traffic, application usage, communication with certain network end points"). EX-1003, ¶279 (citing EX-1001, 7:23-33, 19:67-20:4, 25:46-53, 37:36-61, 68:19-58).

Houghton-Ogawa's data connection C is a "service control link," because it facilitates communication of commands/information relating to control of a service on the mobile terminal, as discussed below. *See, e.g.*, EX-1006, 20, 23; EX-1003, ¶280. In Houghton-Ogawa, "the client may push a message to the server or the server may send a push message to the client" through data connection C shown in Figure 4. EX-1006, 20, 17; EX-1003, ¶280. Messages pushed from push server 401/801 to mobile terminal 404/803 over data connection C ***control*** the target application on the mobile terminal, *e.g.*, by causing the application to start (*e.g.*, "***start to as specified operating state***") or change operating state (*e.g.*, "***change operating state to the state indicated by the message***"). EX-1003, ¶281; EX-1006, 11. "***[T]he push messages may include, for example, a message stimulating, triggering or commanding the launch, display or shift to foreground of a user interface*** feature of the terminal such as an application…" EX-1006, 11, 29 (the push server sends "installation, updates, commands or data messages" to a push application); *see also* discussion *infra* regarding [1a2] (showing that data connection C, the claimed "service control link," supports "control plane communications").

[1a] also requires that the "service control link" be "***provided by the network system***." The '733 specification never describes how a "network system" "provide[s]" a "service control link." EX-1003, ¶282. During prosecution, the examiner rejected this limitation under §112 as indefinite. *See* EX-1002, 99-100. In

response, Applicant argued this limitation "is supported at least by FIG. 16[,] illustrating service control link 1653 communicatively coupling service processor 115 and service controller 122," and the disclosures that "service controller 122…provides for network side of [the] communications with device 100." EX-1002, 76.

Based on Applicant's argument, a POSITA understood that Houghton-Ogawa's "service control link" (data connection C) "is provided by the network system" because (1) data connection C communicatively couples the push server and push client, such that the push server uses transport functionalities associated with data connection C for communications transmitted to or received from push client 405, and (2) before the Critical Date, it was well-known for SSL-based communications between a mobile terminal and a server to be implemented such that both entities participate in maintaining the connection between them after being initiated by the mobile terminal. EX-1003, ¶¶283-284 (citing EX-1006, 18, 20).

[1a1]/[30a1]

The claimed service control link must be "secured by an encryption protocol." Per the '733 specification, encryption protocols that may be used include Transport Layer Security (TLS). EX-1003, ¶285 (citing EX-1001, 17:2-26, 87:62-88:79, 98:42-44; 99:26-29; 101:65-67). The specification uses TLS and Secure Socket Layer (SSL) interchangeably. *See, e.g.*, EX-1001, 98:42-44; 99:26-29; 101:65-67; EX-1003, ¶285.

In Houghton-Ogawa, SSL is used to secure data connection C. *Supra* §§III.A.1, III.A.3(b), III.A.3(e); EX-1006, 20, 18. SSL and its successor TLS were well-known encryption protocols for providing secure communications between entities on a network. EX-1003, ¶286 (citing to EX-1013, 3, EX-1005, 3:61-4:7, EX-1010, 1:38-42). Houghton's data connection C is thus "secured by an encryption protocol," as claimed.

[1a2]/[30a2]

[1a2] requires that the "service control link" be "configured to support control-plane communications between the network system and a service control device link agent on the end-user device." [30a2] recites that the service control link "support[s] control-plane communications" between the "service control device link agent" and a "***network element***."

The same "network element" recited in [30a2] is recited in [30c] and [30d1]. EX-1003, ¶¶287-288. The '733 Patent uses "network element" to encompass any element that is part of a network, *e.g.*, a server. EX-1003, ¶288; EX-1001, 23:46-54, FIGs. 1-8. A POSITA understood that Houghton-Ogawa's push server 401/801—which is a server in claim 1's "network system" (as discussed for [1a])—is also a "network element" as that term is used in the '733 Patent. EX-1003, ¶288.

As discussed for [1a], Houghton-Ogawa's data connection C ("service control link") is how push server 401/801 (within the claimed "network system" in [1a2] and as the "network element" in [30a2]) communicates with push client 405/804 on mobile terminal 404/803 (claimed "end-user device"). EX-1003, ¶289.

A POSITA understood that Houghton-Ogawa's data connection C is "configured to support control-plane communications" as claimed. EX-1003, ¶290. From the '733 specification, a POSITA understood control-plane communications encompass communications "across a network" that "involv[e] supervision" of "device-based" "control" of "service[s]" delivered to a device, for example by "communicating…, controlling, monitoring, or verifying service policy." EX-1003, ¶290; EX-1001, 8:60-9:15, 9:23-24, 37:36-43, 68:19-28.

As discussed for [1a], Houghton discloses that communications between the push server and push client over data connection C include control information related to particular services. EX-1003, ¶291. For example, data connection C facilitates transmission of messages that "cause programs to start to a specified operating state," "change operating state," or "trigger[] or command[] the launch, display or shift to foreground of a user interface." EX-1006, 11; *see also id.*, 14 (controlling information "including the results and responses of messages which the user has replied to by terminal software or web page interaction."), 21-22, 29 (claim 1: the push server sends "installation, updates, commands, or data messages" to a push application); EX-1003, ¶291 (citing EX-1006, 21-22).

Houghton also discloses tailoring what service-related control information is sent based on the ***device*** that the server's push message is being sent to. EX-1003, ¶292. Like the '733 Patent (EX-1001, 8:60-9:15), Houghton describes taking into account, *e.g.,* "user preferences," "network connection preferences," or "security certificates" that a POSITA understood are specific to the user's device. EX-1003, ¶292; EX-1006, 14, 21-22, 29. Houghton also says that actions taken by mobile terminal 404/803 upon receiving push messages may be "***specified in the command C from the server 401***" and determined based on "***user preferences***." EX-1003, ¶293 (citing to EX-1006, 21). For example, the push message may include "information specifying how upon receiving such a message the client 405 will notify and optionally ask the user if the action should be performed," which causes the push client in the mobile terminal to execute "appropriate automated actions and user interface media capabilities… ***as specified in the command C from the server 401***," *e.g.,* "optionally proceed[ing] without audio, with network downloaded audio, or without first requesting confirmation from the user ***as specified by user preferences*** [on the device] and command details." EX-1006, 21. Thus, messages from Houghton's push server are used for device-based control of services delivered to the device in Houghton-Ogawa, and a POSITA understood Houghton-

Ogawa's data connection C is "configured to support control plane communications" as claimed. EX-1003, ¶293.

A POSITA would likewise have understood these communications are "between" the Houghton-Ogawa's push server (which is part of the claimed "network system" in [1a] and the network element in [30a2]) and "a ***service control device link agent*** on the end-user device," as claimed. EX-1003, ¶¶294-296.

The '733 specification does not describe any "service control device link agent." EX-1003, ¶295. It describes a "service control device ***link*** 1691," saying it is a "device side" component that may provide a "solution for transmitting and receiving service policy implementation, control, monitoring and verification information with other network elements." EX-1001, 37:43-62. And it uses the term "agent" to refer to any component—which may be "implemented entirely in software"—that performs some function (*e.g.*, transmitting information for, *e.g.,* "control plane communication"). *Id.*, 15:58-16:2, 42:51-52, claim 26; EX-1003, ¶295. The specification ***does not*** set forth any required function. Moreover, it was well-known that an agent performed function(s) on behalf of an entity (*e.g.*, user, client, server, etc.). EX-1029, 12. This use of "agent" is consistent with Patent Owner's interpretation in litigation. EX-1003, ¶295; EX-1021, 13-23 ("agents" in recited in claim 1 is mapped to "client app[s]" on targeted device(s)); EX-1038, 17.

Houghton-Ogawa's push client 405/804 is "implemented" as "a software run in a processor of the mobile terminal 404." EX-1006, 16. As discussed above, it facilitates communications with the push server using data connection C, and is used for transmission, controlling, and execution of a service on the device on the server's behalf. EX-1003, ¶296; EX-1006, 21, FIG. 4. Houghton-Ogawa's push client 405/804 is thus the claimed "service control device link agent." EX-1003, ¶296.

[1b]/[30b]

The claimed end-user device must have "a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus," with "each of the plurality of device agents identifiable by an associated device agent identifier."

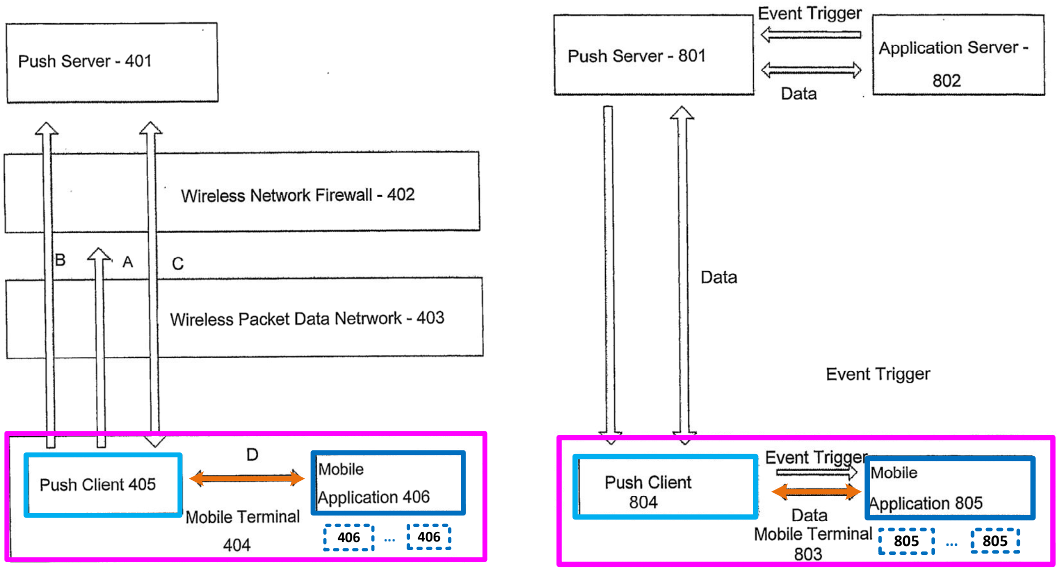
As discussed for [1a2], the '733 Patent uses the term "agent" to include a "component" implemented "entirely in software" that performs some function on behalf of a client or server. A "***device*** agent" is an agent on a device. EX-1003, ¶297.

In Houghton-Ogawa, push client 405/804 is communicatively coupled to multiple mobile applications 406/805. EX-1003, ¶298; EX-1006, 21. Houghton discloses various examples of such applications, including, *e.g.*, "video game" and "messaging" applications described below. *See* discussion for claims 15 and 20.

Houghton-Ogawa's mobile applications may be "***direct[ed]***" by a push server (using a push message) to perform functions related to the service, including "use of additional network resources either on the push server or other server" and "application data transfer." EX-1006, 21. Because multiple mobile applications on the mobile terminal are implemented in software and each performs functions directed by and thus on behalf of, *e.g.*, an application server providing the user a service, a POSITA understood these mobile applications constitute "a plurality of device agents," as claimed. EX-1003, ¶299.

A POSITA would have likewise understood that push client 405/804 is communicatively coupled to these device agents "through an agent communication bus," as claimed. EX-1003, ¶300.

Specifically, push client 405/804 may "pass… command details" to specific mobile applications, and "accept data D from each of a plurality of mobile applications 406." EX-1006, 21, FIG. 4.



EX-1006, Figure 4 (annotated, left); Figure 8 (annotated, right)

The arrows from Houghton Figures 4 and 8 above (highlighted orange) represent data communications in the mobile terminal between push client 405/804 and mobile applications 406/805. EX-1003, ¶¶301-302. A POSITA understood that such communications would be "through an agent communication bus" as that term is used in the '733 patent. EX-1003, ¶302 (explaining that the specification uses "agent communication bus" to include a communication link that facilitates communications between device agents); EX-1001, 42:48-58; EX-1038, 24.

Alternatively, a POSITA would have had reason to implement the communication link between Houghton's push client and mobile applications in Houghton-Ogawa as a bus. EX-1003, ¶303. Before the Critical Date, it was well-known to use a communication bus (*e.g.*, a "D-bus") to facilitate communications ("D") of the application-specific messages between the push client and the destination applications, as Houghton describes. *Id.* (citing EX-1031, 10:56-62, EX-1008, ¶28, FIG. 4). Using such a bus in Houghton's mobile terminal would have been a conventional, obvious way to implement what Houghton describes, and involves utilizing familiar, known components (a bus) to achieve a predictable result of facilitating Houghton's push client and mobile applications to interface with one another. EX-1003, ¶303. A POSITA would have reasonably expected success doing so. *Id*. Houghton-Ogawa's end-user device (mobile terminal 404/803) thus has "a plurality of device agents communicatively coupled to the service control device link agent through an agent communication bus," as claimed. *Id.*

Each of Houghton-Ogawa's "device agents" is "identifiable by" an "associated device agent identifier," as claimed. EX-1003, ¶¶304-306.

The '733 specification does not describe requirements for the claimed "associated device agent identifier." EX-1003, ¶305. In Houghton-Ogawa, push messages are routed by the push client to specific mobile applications using "binary or text information" in the message that "specif[ies] which mobile application 406 from a plurality of such applications" is the target of the push message. EX-1006, 21. A POSITA understood that the "information specifying which mobile application 406" to send messages to, as Houghton teaches, meant that each of Houghton-

Ogawa's "device agents" was "identifiable by" an "associated device agent identifier," as claimed. EX-1003, ¶305.

Alternatively, implementing Houghton's information specifying a particular application to be in the form of an "identifier" would have been a conventional and obvious way to implement what Houghton describes (EX-1006, 21), and involves utilizing a known technique (use of application identifiers) to a known system (Houghton's push-based server-client system) to achieve a predictable result of accurately routing messages to applications based on their identifiers, as suggested by Houghton and as was well-known before the Critical Date. EX-1003, ¶306 (citing EX-1008, ¶22). A POSITA would have reasonably expected success doing so. EX-1003, ¶306.

[1c]

Houghton-Ogawa's mobile terminal includes memory that stores Ogawa's shared encryption key (*supra* §III.A.3(d)), which as discussed *supra* §III.A.3(e), secures Houghton-Ogawa's data connection C with Houghton-Ogawa Message Encryption. EX-1003, ¶¶307-308; *cf.* EX-1001, 87:57-88:7 (describing "two or three layers of encryption"). Houghton-Ogawa's end-user device thus includes "memory configured to store an encryption key," as claimed. EX-1003, ¶¶308 (citing EX-1006, 29, 22).

Additionally, ***under Patent Owner's claim interpretation*** in litigation, the "encryption key" limitations recited in [1c], [1c1]/[30c], and [1d2]/[30d2] may be ***part of*** the "encryption protocol" that secures limitation [1a1]'s service control link. EX-1021, 3-13 and 24-23 (using the same features of the "security protocols" used in the alleged product to allege infringement of "encryption protocol" in [1a1] and "encryption key" in [1c]); EX-1038, 8, 29. In other words, Patent Owner asserts the "encryption key" limitation is satisfied by systems where encryption is performed using SSL (or similar) "encryption protocol" without an additional layer of encryption. *Id.* As discussed below, Houghton-Ogawa also separately meets the claims even if the limitations recited in [1c], [1c1]/[30c], and [1d2]/[30d2] are interpreted to encompass encryption performed ***as part of*** a SSL-enabled encryption protocol that also meets limitation [1a1] (*i.e.*, single-layer encryption). *See Nidec*, 868 F.3d at 1017; 83 Fed. Reg. 51, 340, at 51, 353.

Under Patent Owner's interpretation, Houghton-Ogawa's memory meets [1c], because, as noted for [1a1], Houghton-Ogawa's data connection C is secured using SSL. EX-1003, ¶¶309-311; *supra* §§III.A.3(b); III.A.3(e). While Houghton does not describe the details of how SSL is implemented, before the Critical Date, it was well-known that SSL/TLS uses ***symmetric*** encryption that involves using the ***same*** key at the source and destination of a message for encryption and decryption.

EX-1003, ¶311 (citing EX-1013, EX-1014, EX-1026). A POSITA likewise understood that such keys were conventionally stored in the respective memories of the encrypting and decrypting entities. EX-1003, ¶311. Thus, under Patent Owner's claim interpretation—which reads the claims onto systems that ***only*** secure client-server communication channels based on the symmetric encryption used in SSL/TLS—Houghton-Ogawa, which uses SSL (*supra* §§III.A.1, III.A.3(b), III.A.3(e)), includes "memory configured to store an encryption key." EX-1003, ¶311.

[1c1]/[30c]

[1c1] requires that the encryption key be "shared between the service control device link agent" (Houghton-Ogawa's push client 405/804, as discussed for [1a2]) "and a service control server link element of the network system." [30c] recites that the encryption key be "shared between the service control device link agent" and "the network element" (Houghton-Ogawa's push server, as discussed for [30a2]).

While the '733 specification never describes element [1c1]'s "service control server link element of the network system," it refers to a "service control server ***link*** 1638," and says it is a "network side" component that may "provide[] an efficient and secure mechanism for transmitting and receiving service policy implementation, control, monitoring and verification information between the device agents (*e.g.*, service processor agents/components) and other network elements (*e.g.*, service controller agents/components)." EX-1001, 68:19-40; EX-1003, ¶¶312-313.

As discussed for [1a], push server 401/801 is part of Houghton-Ogawa's "network system." A POSITA understood that Houghton-Ogawa's push server "provides a mechanism for transmitting and receiving" "service policy… information" between "device agents" and other "network elements," because: (1) Houghton discloses data connections between push server 401/801, push client 405/804 on mobile terminal 404/805, and application server 802 (EX-1006, FIGs. 4 and 8), (2) Houghton describes using those data connections to "establish[]" "a data connection" "between" the "application server" and "mobile application" (*id.*, 23), (3) Houghton describes "redirection" of data received from the mobile applications on the mobile terminal "***to other servers***" via the push server (*id.,* 21), and (4) as discussed for [1a2] and for [1e], Houghton's connections are used for control-plane communications between Houghton-Ogawa's application servers and mobile applications. EX-1003, ¶314 (EX-1006, 21-22). A POSITA would thus have understood that Houghton-Ogawa's push server is a "service control server link element of the network system," as recited in [1c1]. EX-1003, ¶314.

In Houghton-Ogawa, Ogawa's encryption key is stored on the mobile terminal to enable the push client to decrypt data received from the push server on which the same encryption key is also stored. *Supra* §III.A.3(d); EX-1005, 5:59-65, 6:64-7:21, 9:16-34. As discussed *supra* §III.A.3(d), before the Critical Date, this was well-known for symmetric encryption. EX-1003, ¶315 (citing EX-1009, 3:25-27, 8:3-5; EX-1013, 3).

First, a POSITA understood that the same key stored at Houghton-Ogawa's mobile terminal and push server for Houghton-Ogawa Message Encryption—which is used by both Houghton-Ogawa's push client ("service control device link agent") and push server ([1c1]'s "service control server link element of the network system" and [30c]'s "network element") for encryption/decryption—was "***shared between***" those claimed components. EX-1003, ¶316.

Additionally and alternatively, a POSITA would have understood that ***<u>under Patent Owner's claim interpretation</u>***—which covers systems that only secure client-server communications using the single layer of symmetric encryption used in SSL/TLS—the key for Houghton-Ogawa's symmetric SSL encryption (*supra* §§III.A.1, III.A.3(b), III.A.3(e)), by being stored temporarily at both the mobile terminal (with the push client) and the push server, was likewise "shared between" the push client and push server. EX-1003, ¶317.

[1d1]/[30d1]

[1d1] requires the "service control device link agent" to be "configured to: receive, over the service control link, an encrypted agent message from the service control server link element." [30d1] recites "receiving" an encrypted agent message from claim 30's "network element."

In Houghton-Ogawa, push client 405/804 (claimed "***service control device link agent***") is configured to receive, over data connection C (claimed "***service control link***"), encrypted messages from the push server (claimed "***service control server link element***" in claim 1 in [1c1], and "***network element***" in claim 30). EX-1003, ¶¶318-319.

The '733 specification never uses the term "encrypted agent message." Based on the plain claim language, a POSITA would have understood the term to encompass an encrypted message sent to an agent. EX-1003, ¶320. In Houghton-Ogawa, messages are encrypted both using Houghton-Ogawa Message Encryption and an SSL encryption protocol before being transmitted to the push client. *Supra* §§III.A.3(b), III.A.3(e).

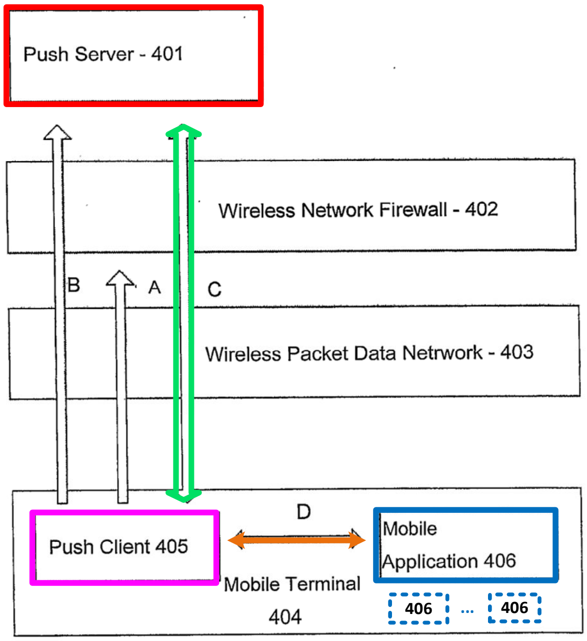
First, because the messages are encrypted using Houghton-Ogawa Message Encryption, a POSITA understood that, in Houghton-Ogawa, the service control device link agent is "configured to" "receive, over the service control link, an encrypted agent message from the service control server link element," as claimed in claim 1 and that the message is received "from a network element," as claimed in claim 30. EX-1003, ¶321.

Additionally and alternatively, ***under Patent Owner's claim interpretation***—which covers systems with only the single layer of symmetric encryption used in SSL/TLS—Houghton-Ogawa's symmetric SSL encryption (*supra* §§III.A.1, III.A.3(b), III.A.3(e)) alone also meets limitations [1d1] and [30d1], because SSL is a protocol for encrypting messages sent over the data connection to Houghton-Ogawa's push client. EX-1003, ¶322.

[1d2]/[30d2]

The claims require the service control device link agent to (or be configured to) "us[e]" the "encryption key" to "obtain[]" a "decrypted agent message." EX-1003, ¶323. Based on the plain claim language, a POSITA would have understood "decrypted agent message" to encompass a message sent to an agent that has been decrypted. *Id.*

Per Houghton, "[u]pon receiving… a message, ***appropriate automated actions*** and user interface media capabilities of the mobile terminal ***as specified in the command C*** from the server 401 ***are executed by the push client 405***," *e.g.*, "passing the command details (arrow D) to the specified mobile application, module or additional feature within the same application suite," "launching the application, module or feature," etc. EX-1006, 21.



EX-1006, FIG. 4 (annotated)

In Houghton-Ogawa, encrypted messages (*e.g.*, received from the application server via the push server) are decrypted at the push client, which is implemented to use Ogawa's decrypt unit and shared encryption key to decrypt messages that were encrypted using Houghton-Ogawa Message Encryption. *Supra* §§III.A.3(b)-III.A.3(d); EX-1003, ¶¶324-325. A POSITA understood that the push client decrypts the message ***before*** executing the actions specified by the message to process the message and determine what actions need to be taken. EX-1003, ¶325; *see also* EX-1006, 34 ("***[T]he push client*** and push server establish a secure connection and ***unwrap such security***" on the application's behalf); EX-1005, 5:59-67, 6:64-7:21, FIG. 7. A POSITA understood that, in Houghton-Ogawa, the service control device link agent is thus configured to "us[e] the encryption key" of Ogawa to "obtain a decrypted agent message," as claimed. EX-1003, ¶325.

Additionally and alternatively, ***<u>under Patent Owner's claim interpretation</u>***—which covers systems with only a single layer of symmetric encryption used in SSL/TLS—Houghton-Ogawa's symmetric SSL encryption (*supra* §§III.A.1, III.A.3(b), III.A.3(e)) alone also meets limitations [1d2] and [30d2], because messages encrypted using SSL must be decrypted using the same encryption key used to encrypt the message, thereby obtaining a message for the agent that has been decrypted, *i.e.*, "a decrypted agent message" (under Patent Owner's interpretation). EX-1003, ¶326 (citing EX-1009, 6:59-7:17, 7:34-40, 8:1-5).

[1d3]/[30d3]-[30d4]

The claims require that the "decrypted agent message" include "a particular agent identifier and message content for delivery to a particular device agent of" the "plurality of device agents" where "the particular agent identifier identif[ies] the particular device agent."

In Houghton-Ogawa, the push client (claimed "***service control device link agent***") receives encrypted ***messages*** from the push server (as discussed for [1d1]) and decrypts it (as discussed for [1d2]) to obtain "decrypted agent message[s]," as claimed. The push client uses the information included in the message, including "information specifying which mobile application 406 from a plurality of such applications" ("***plurality of device agents***," as discussed for [1b]) the message is directed to, to push the message to the appropriate mobile application. EX-1006, 21; EX-1003, ¶¶327-328.

As discussed for [1b], a POSITA understood that Houghton-Ogawa's "information specifying which mobile application" to route the message to is, or would have been obvious to implement as, an "associated device agent identifier." EX-1003, ¶329. A POSITA would have likewise understood that this information is also a "particular agent identifier" in Houghton-Ogawa's "decrypted message" that "identifies the particular device agent" to which the message should be delivered. *Id*.

Houghton-Ogawa's message also includes "binary or text information to be passed to the… specified mobile application," which, as further explained for [1e] *infra*, a POSITA understood (based on Houghton's teachings) to constitute message content and commands that are used by the application to execute and display content. EX-1003, ¶330 (citing EX-1006, 21); *see also* EX-1006, 8 (indicating that "rout[ing] commands or application-specific data to the mobile application" was conventional). EX-1003, ¶330 (noting that the '733 specification never uses the term "message content.").

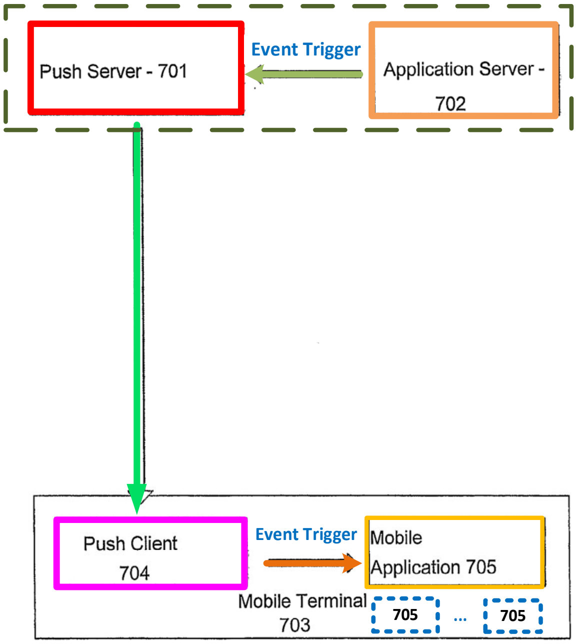
[1e]/[30e]

[1e] requires the "message content" to be "from a particular server of a plurality of servers communicatively coupled to the service control server link element." EX-1003, ¶331. [30d1] recites that the "plurality of servers" be "communicatively coupled to" claim 30's "***network element***."

Houghton-Ogawa's push server is the "service control server link element" in claim 1 (as discussed for [1c1]), and "network element" in claim 30 (as discussed for [30a2]). The "binary or text information," "commands," and "application-specific data" in Houghton-Ogawa's received message is "message content" as discussed for [1d3]. EX-1003, ¶332.

Houghton discloses an ***application server*** sending message content to the push server, which triggers the push server to push the message to the push client on the mobile terminal, and ultimately to a mobile application on the mobile terminal. EX-1003, ¶333; (citing EX-1006, 21-22). "Figure 7 illustrates an example of an 'COMMAND PUSH' procedure" that a POSITA understood to be implemented in Houghton's Figure 4 system "wherein [Houghton's] ***push server***... is ***triggered by a trigger event*** as for example ***from an application server***… to push an application command message to the push client… and thereby initiate a mobile terminal client trigger event in a mobile application… from a plurality of such applications… on the terminal…" EX-1006, 21-22. "***The trigger [event]*** mechanism ***may***

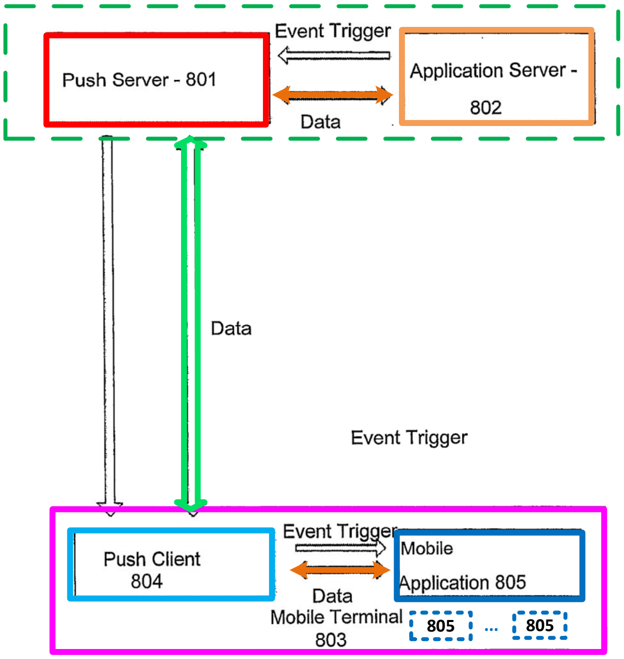
be… an IP-triggered ***application launch and data transfer*** as in the case of mobile application launched by contact to a specified IP port." *Id.* "***The trigger event***" "may optionally ***include commands*** or data affecting the aspect of visual presentation of mobile application…" *Id.* Figure 7, annotated below, shows that push client 704 delivers to mobile application 705 data of trigger event included in the message that the push server 701 received from application server 702. EX-1003, ¶333.



EX-1006, Figure 7 (annotated)

A POSITA understood that "event trigger" messages sent from the application server to the push client includes content, *e.g.*, a command to launch or use particular mobile applications such as a display or audio application, that constituted "message content," as claimed. EX-1003, ¶334.

A POSITA would also have understood that Houghton discloses message content being sent from the application server to a mobile application through the "data connection" between the two. EX-1003, ¶335 (citing EX-1006, 9). Houghton emphasizes that the connection between the application server and the application on the mobile terminal is a "data connection" for transmitting data. EX-1003, ¶335; EX-1006, 23.



EX-1006, Figure 8 (annotated)

Finally, a POSITA understood Houghton to disclose that the illustrated application server is one of multiple servers in communication with the push server. EX-1006, 22 ("push server 401 [can direct a message] ***to other servers***"); EX-1003, ¶336.

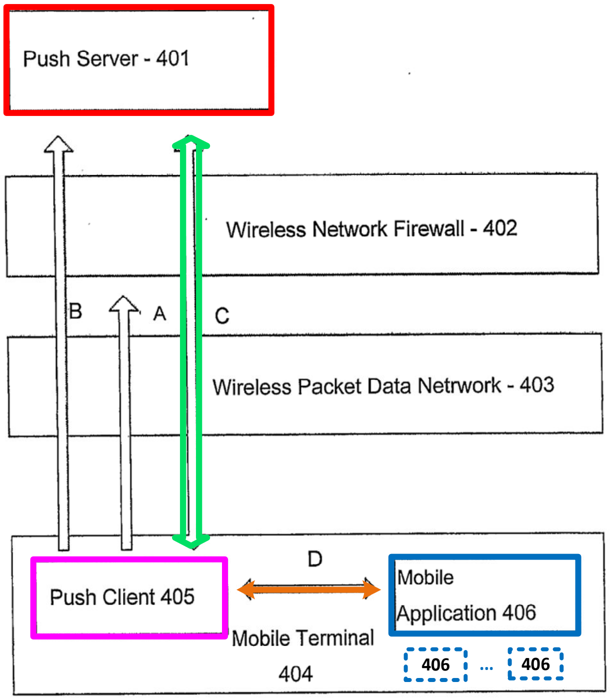
Moreover, based on Houghton's express disclosure of examples of application servers—e.g., a telecommunication service server, gaming environment server—a POSITA understood Houghton to include multiple application servers, *e.g.*, with each application server providing a particular service, and sending messages or event triggers corresponding to that particular service. EX-1003, ¶337 (citing EX-1006, 14). Alternatively, such an implementation would have been a conventional and obvious way to implement what Houghton describes, and involves utilizing familiar, known components (multiple individual application servers corresponding individual services associated with individual mobile applications) to achieve a predictable result of providing a variety of services to a user through applications on a mobile terminal. EX-1003, ¶337.

[1f]/[30f]

The claims require that the "service control device link agent" be "configured to," "deliver[] the message content to the particular device agent over the agent communication bus" "based on the particular agent identifier." EX-1003, ¶338.

As discussed for [1b] and [1d3], the push message received from Houghton-Ogawa's push server includes "information ***specifying which mobile application 406*** from a plurality of such applications" to "pass[]" the push message's content to. EX-1006, 21. "Upon receiving such a message, appropriate automated actions… as specified in the command C from the server 401 are ***executed by the push client 405***," for example "***passing the command details (arrow D) to the specified mobile application***." *Id*. Indeed, delivering message content based on the application identifier that was included in the push message was conventional even before Houghton. EX-1003, ¶339 (citing EX-1006, 8, 22, 5; EX-1008, ¶28).

A POSITA also understood that such communication would occur "through the agent communication bus" (discussed for [1b]). Houghton-Ogawa thus meets this element. EX-1003, ¶340.



EX-1006, FIG. 4 (annotated)

(b) Claim 2

Per claim 2 claim 1's "particular server" may comprise "a service download control server" or "a content management server."

The '733 specification uses "service download control server" to encompass a server that "provides a download function to install and/or update service software elements." EX-1001, 77:31-38. The '733 specification does not describe a "content management server," but a POSITA understood "content management" encompassed managing any aspect of delivery of data to an end-user. *Id.*, 16:53-54; EX-1003, ¶¶341-342.

Houghton teaches an application server triggering the pushing of "application installation, updates, commands, or data messages" in a message from the push server to the push client. EX-1003, ¶343; EX-1006, 29. Thus, Houghton-Ogawa's application server comprises "***a server download control server***" by providing a download function to install and/or update service software elements, and "***a content management server***" because it manages or controls the delivery of data to the push client (and the mobile application). EX-1003, ¶343 (citing EX-1001, 77:31-38).

Houghton also says an application server can trigger the push server "to ***push an application command message*** to the push client." EX-1006, 21-22. The application server is "***a separate server***" that "***notif[ies] the [push] server directly***

of events or messages to be sent*.**" EX-1006, 14; *see also*, 22 ("The ***trigger mechanism… may be an IP-triggered application launch and ***data transfer***…). For this additional reason, Houghton-Ogawa's application server comprises "***a content management server***." EX-1003, ¶344.

(c) Claim 5

Claim 5 requires claim 1's "message content" to be "based, at least in part, on a user preference." Houghton says the push server may, based on "***user preferences*** stored in… the push server," "request the push client… to display or otherwise… notify the user asking permission for launching [a] mobile application… prior to application launch." EX-1006, 22. Houghton also discloses the "content" of this user notification being "configured on" the push server "***based on*** the service and ***preferences of the individual*** receiving the message." *Id.*; EX-1003, ¶345. Thus, in Houghton-Ogawa, the message content sent from the push server is "based on" "user preference[s]," *e.g.*, preferences regarding how the user likes to be notified. EX-1003, ¶345.

(d) Claim 7

Claim 7 requires claim 1's "message content" to "comprise[]" "a service offer" or "an advertisement."

The '733 specification does not use the term "service offer," but a POSITA would have understood it to encompass offering a choice about whether to accept a service. EX-1003, ¶¶346-347. As discussed for claim 5, Houghton discloses message content from the push server that comprises information ultimately displayed to a user, *e.g.,* a notification asking user's permission to display or launch an application. EX-1006, 11-12, 22 ("[P]ush messages may include" "notification providing event information from which the user may ***select or decline*** to display the application.") EX-1003, ¶348 (citing EX-1006, 22, which provides example mobile applications that provide different services). A POSITA understood that a notification allowing a user to ***select or decline*** to display a mobile application is an ***offer*** to receive a ***service*** through one of Houghton's various mobile applications, which the user may accept or decline. EX-1003, ¶349.

Separately, Houghton discloses using its push message system for "mobile electronic commerce." EX-1006, 22. A POSITA would have understood that Houghton thus discloses transmission of advertisements, because advertisements were conventionally a major feature of mobile electronic commerce implementations. EX-1003, ¶350 (citing EX-1033, EX-1034). Alternatively, an implementation in which Houghton's push system was used to transmit advertisements as part of its disclosed mobile electronic commerce application (EX-1006, 22) would have been conventional and well within a POSITA's skill to implement. EX-1003, ¶350. Houghton discloses its push messages including media or multimedia such as pictures, video, or audio. EX-1006, 14. Before the Critical Date, it was well-known to push digital advertisements in these media formats as part of mobile electronic commerce services, using, *e.g.*, communication protocols like WAP (*see* EX-1006, 1, 5, 9). EX-1003, ¶350 (citing EX-1015, [0012], which discusses pushing "advertising image data" to "mobile terminal[s]" using "WAP"). Thus, using Houghton's push system in Houghton-Ogawa to push advertisements would have involved utilizing familiar, known components (pushed message content, digital advertisements) to achieve a predictable result of facilitating use of Houghton's push messaging system in the context of a mobile electronic commerce system, and a POSITA would have reasonably expected success doing so. EX-1003, ¶350; EX-1006, 22.

(e) Claim 8

Claim 8 requires claim 1's "message content" to "comprise[] information from a third party configured to provide control of a service or a billing for a service." As discussed for claim 2, Houghton-Ogawa's application server comprises a content management server and a service download control server.

A POSITA understood that Houghton-Ogawa's application server controls aspects of services delivered to a mobile terminal because it controls what data is pushed to the push client as message content—*e.g.*, service content, or updates to the application providing the service to the user. EX-1003, ¶¶351-352; *see supra* regarding claim 2. Thus, data received by the push server from Houghton-Ogawa's application server that is pushed as message content to the client includes information "configured to provide control of a service," as claimed.

Further, a POSITA understood that data from the application server constitutes "information from a ***third party***" because the application server is separate from Houghton-Ogawa's push server, and the '733 Patent characterizes servers coupled to the service control server link element as providing "third party" function. EX-1003, ¶353 (citing EX-1001, 77:39-47, FIG. 16).

(f) Claim 9

Claim 9 requires claim 1's "message content" to "comprise," *e.g.*, "a software update." EX-1003, ¶354. Houghton says messages transferred from the push server to the mobile terminal can include "application[] updates to replace or improve installed applications." EX-1006, 9, 34 (claim 29), 31 (claim 15). A POSITA understood such application updates are "***software updates***," as claimed. EX-1003, ¶354 (citing EX-1006, 11-12).

(g) Claim 10

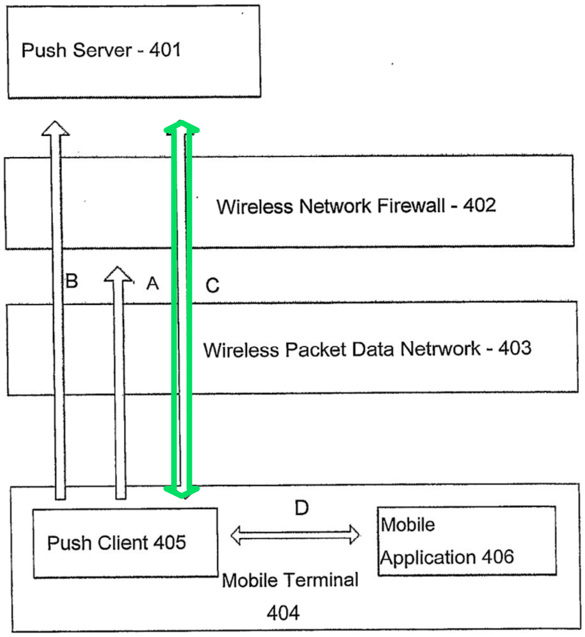
Claim 10 requires the "message content" to "comprise[] software or a media file." As discussed for claim 9, in Houghton-Ogawa, application updates are sent using Houghton's push system. A POSITA understood "software updates" comprise "software," as claimed. EX-1006, 9, 29, 31 (claim 15), 34 (claim 29); EX-1003, ¶355.

Additionally, Houghton discloses message content directed to media-based applications (*e.g.*, picture transfer, mobile gaming, multimedia interactivity, messaging). EX-1006, 21-22. Because the push message is application-specific (*see supra* [1b]) and the applications can be media-based, a POSITA understood that message content directed to such applications included media files. EX-1003, ¶356 (citing EX-1006, 11-12; EX-1015, [0012]).

(h) Claim 13

Claim 13 requires the "service control device link agent" (Houghton-Ogawa's push client) "is further configured to send a device message to the service control server link element" (Houghton-Ogawa's push server) "over the service control link" (Houghton-Ogawa's data connection C). EX-1003, ¶357. The '733 specification does not use the term "device message," but based on the claim's plain language, a POSITA understood the term to encompass any message from a device on the network, *e.g.,* the end-user device. *Id.*

Per Houghton, "the [push] client may push a message to the [push] server" through connection C. EX-1006, 20; EX-1003, ¶358.



EX-1006, FIG. 4 (annotated)

A POSITA understood that a message from the push client on the mobile terminal was a "device message," as claimed. EX-1003, ¶359.

(i) Claim 14

Claim 14 requires claim 13's "device message" to "comprise[] a service usage report or an integrity report." EX-1003, ¶360.

As discussed for claim 10, messages sent from the push server to the push client in Houghton-Ogawa may include a media file and/or instructions to change the state of the destination application presented on a user interface. A POSITA understood that presenting such content to a user on the user interface of a mobile terminal constitutes usage of a service. *Id.*

Houghton says that after executing a function in response to push message received from the push server—*e.g.*, presenting the received media file or changing the state of the destination application (EX-1006, 11-12, 22)—"client 405 may also send a message to the server 401 (step 633), such as ***a command execution acknowledgement or result***." EX-1006, 26. Because this message from the mobile terminal includes information about the acknowledgement or result of executing the command for a particular service, it constitutes the claimed "service usage report." EX-1003, ¶¶361-363.

Houghton also discloses its mobile terminal sending messages to the push server to "maintain[] an open path for network communication with the server." EX-1006, 15. The message "keeps the connection to the server open and ***tests the integrity of the connection***." *Id*. A POSITA understood that this message constitutes an ***integrity report*** because the message provides information regarding the integrity of the connection between the client and server, and "upon failure to receive acknowledgement of" such a message, "the push client or the push server" "may choose to open a new connection." *Id*., 30; *see also id*., 11; EX-1003, ¶¶364-365.

(j) Claim 15

Claim 15 requires claim 13's "device message" to "comprise[] a user response." As discussed for claim 13, Houghton discloses a device message pushed from the mobile terminal to the push server. A POSITA understood—in the context of client-server environments—that messages from the mobile terminal conventionally included user responses to previously-received messages from the push server. EX-1003, ¶366.

Houghton teaches "client-side events" such as "***video game actions or events, [and] messaging actions***" that Houghton's "***push client makes the server aware of***." EX-1006, 14. A POSITA understood or found obvious that such information sent by the push client would be sent as content in messages from the mobile terminal. EX-1003, ¶¶_ (citing EX-1006, 1). A POSITA would also have understood that "video game actions or events" and "messaging actions" are examples of a "***user response***," as claimed, because they are sent by the push client in response to a user's action on the mobile terminal when using, *e.g.*, a "video game" or "messaging" application. EX-1003, ¶367. They are thus "device message[s]" that "comprise a user response," as claimed. *Id.*

Additionally, Houghton says the push server may receive messages from another server that "notif[ies] the [push] server directly of events or messages to be sent [to the push client]." EX-1006, 14. Such triggering messages can include "responses of messages which ***the user has replied to*** by terminal software or web page interaction." *Id.*; EX-1003, ¶368.

(k) Claim 19

Claim 19 requires the "end-user device" (Houghton-Ogawa's mobile terminal) to include "a user interface," and requires "the particular device agent" (*e.g.,* a "video game" or "messaging" application) to be "configured to assist in presenting a notification through the user interface, the notification being based on the message content." EX-1003, ¶369.

Houghton's mobile terminal in Houghton-Ogawa has a user interface. *E.g.,* EX-1006, 11-12; EX-1003, ¶370. Houghton discloses "[i]n response to receiving [a push] message, a mobile terminal may… ***open…user interface feature of the terminal thereof to a designed application view*** or location, ***present new information of the availability of new information, a new feature or operating state***." EX-1006, 11-12. Houghton's application thus aids in presenting ("***is configured to assist in presenting***") information ("***a notification***") "regarding new information[,] feature, or operating state" for the application through the user interface, in a way that is specified in Houghton's application-specific message ("***based on the message content***"). *See supra* [1d3]; EX-1003, ¶370.

(l) Claim 20

[20a]

Claim 20 requires that "the particular device agent" (*e.g.,* Houghton-Ogawa's "video game" or "messaging" application) is configured to "assist in obtaining a user response to the notification" in claim 19. EX-1003, ¶371.

As discussed for claim 19, the mobile applications in Houghton-Ogawa—*e.g.,* a "video game" or "messaging" application—are configured to assist in presenting "new information" received from the network, through the user interface on Houghton-Ogawa's mobile terminal. EX-1003, ¶372. And as discussed for claim 15, Houghton-Ogawa's push client is configured to send to the push server "video game actions or events" and "messaging actions" which are examples of "user response[s]" that correspond to a user's action on the mobile terminal when using, *e.g.*, a "video game" or "messaging" application. *Id.*

A POSITA understood that user actions on a "video game" or "messaging" application in Houghton-Ogawa would have included actions made in response to the presented notifications while using the "video game" or "messaging" application. EX-1003, ¶¶373-374. This is because a POSITA understood that the "game actions" (*e.g.*, user response to another user's chess move) or "messaging actions" (*e.g.*, user response to another user's message or an alert) would have included responses to the "new information" (the claimed "notification") that was presented to the user on the application. EX-1003, ¶374 (citing EX-1028, 729-730). A POSITA understood that this would have met the requirement of "assist[ing] in obtaining a user response to the notification" for two reasons.

First, a POSITA understood that because the application assists with presenting "new information" that leads to the user's reaction/response, the application assists in obtaining the user's response to the notification. EX-1003, ¶375.

Second, a POSITA had several reasons to implement the user's response in Houghton-Ogawa to be submitted through the same application that presented the "new information." EX-1003, ¶376. Implementing presentation of new information and obtaining user responses to that information in one application would have (1) improved processing speed, (2) reduced traffic between separate device applications that would otherwise need to interact to perform both functions, and (3) reduced security risk that would otherwise be introduced due to the communications between the separate device components. *Id*. A POSITA would have reasonably expected success with such an implementation because it was commonplace to implement applications to utilize a user interface for presenting information to and receiving input from a user. *Id.*

[20a] also requires "the particular device agent" (Houghton-Ogawa's mobile application) be configured to "send a first message to the service control device

link" agent (Houghton-Ogawa's push client), where "the first message compris[es]" a "user response." Houghton teaches that its mobile application can send messages to the push client, which sends the message to the push server. EX-1006, 21; EX-1003, ¶377; *see also* EX-1006, 14, 32; *see also* discussion *supra* regarding claim 15. Houghton also teaches that the message can "include an alarm [or] notification" received from the mobile terminal. EX-1006, 21. A POSITA understood that in the context of a video game or a messaging application, such alarm or notification can include the user's response (*i.e.*, "user's actions" discussed above) when using the application. EX-1003, ¶377 (citing EX-1028).

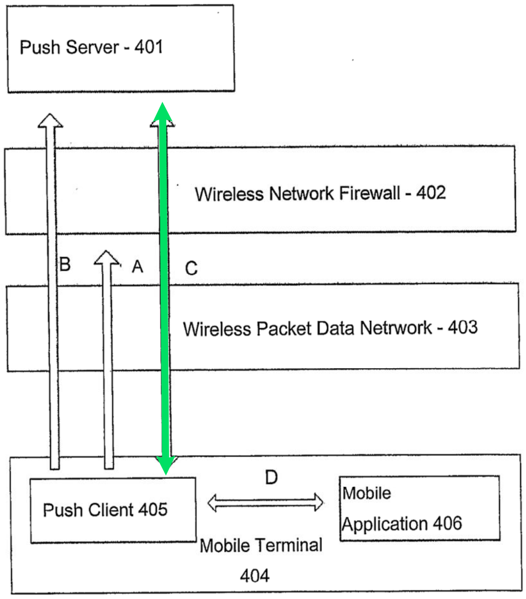
[20b]

[20b] requires that the "service control device link agent is further configured to: using the encryption key, generate an encrypted device message comprising the user response, and send the encrypted device message to a service control server link element over the service control link." EX-1003, ¶378.

As discussed for claim 15, Houghton discloses "client-side events"—*e.g.,* "video game actions or events, [and] messaging actions"—that the "push client makes the server aware of." As also discussed there, messages sent by the mobile terminal's push client to the push server containing this information are "device message[s]" that "comprise a user response." EX-1003, ¶378.

As discussed for, *e.g.,* [1c]-[1c1], Houghton-Ogawa's push client ("***service control device link agent***"), is configured to decrypt encrypted messages received from Houghton-Ogawa's push server ("***server control server link element***") through data connection C ("***service control link***"). EX-1003, ¶379; *see supra* §III.A.1. As also described for [1c]-[1c1], Houghton-Ogawa uses symmetric Houghton-Ogawa Message Encryption, where Ogawa's shared key ("***encryption key***") is stored at multiple network entities and used for encrypting and decrypting messages/content sent from one network entity to another. EX-1003, ¶379. As discussed *supra* §III.A.3(d), a POSITA had reason to implement Houghton-Ogawa's mobile terminal to encrypt data that it transmitted to other network entities, and thus a POSITA understood that messages transmitted from Houghton-Ogawa's push client to the push server were encrypted, where the push client on the mobile terminal used the same symmetric encryption scheme discussed for claim 1 to achieve device-side encrypting. EX-1003, ¶379. Thus, Houghton-Ogawa meets [20b]. *Id.*

Additionally and alternatively, this limitation is met ***under Patent Owner's claim interpretation***—which covers systems that only secure client-server communications using TLS/SSL symmetric encryption. EX-1003, ¶380. As discussed for, *e.g.,* [1c]-[1c1], it was well-known to symmetrically encrypt and decrypt a message transmitted through SSL protocols, and Houghton discloses two-way communications (arrow C) between the push server and push client that are secured using SSL. EX-1006, 20; *see* discussion regarding claims 13, 15. A POSITA would have implemented symmetric encryption/decryption for transmission of a message ***from*** the end-user device ***to*** the server through the ***same*** SSL-secured connection for the same reasons that would have motivated a POSITA to use symmetric encryption/decryption for messages transmitted in the other direction (discussed for claim 1). EX-1003, ¶380 (citing EX-1009, 6:59-7:16, 8:1-5).



EX-1006, FIG. 4 (annotated)

(m) Claim 21

Claim 21 requires claim 1's "service control link" (data connection C) to "support[] asynchronous transmissions" by the "service control server link element" (Houghton-Ogawa's push server). From the '733 disclosure, a POSITA understood that the term "asynchronous transmissions" encompasses transmissions by a server sent to a client in response to a request from the client. EX-1003, ¶381 (citing EX-1001, 38:19-32, 69:23-24).

In Houghton-Ogawa, the push server can transmit messages ***asynchronously*** because the messages can be sent out in response to receiving a trigger event from the push client. EX-1003, ¶382. As discussed for claim 15, the messages may be pushed in response to a "client-side event" such as a user device's request, which is akin to the user request disclosed in the '733 patent. *Id.* (citing EX-1006, 14). Accordingly, in Houghton-Ogawa, data connection C ("***service control link***") supports asynchronous transmission by the push server after the server receives a user request, consistent with how this term is used in the '733 specification. EX-1003, ¶382 (citing EX-1001, 38:19-32, 69:23-24).

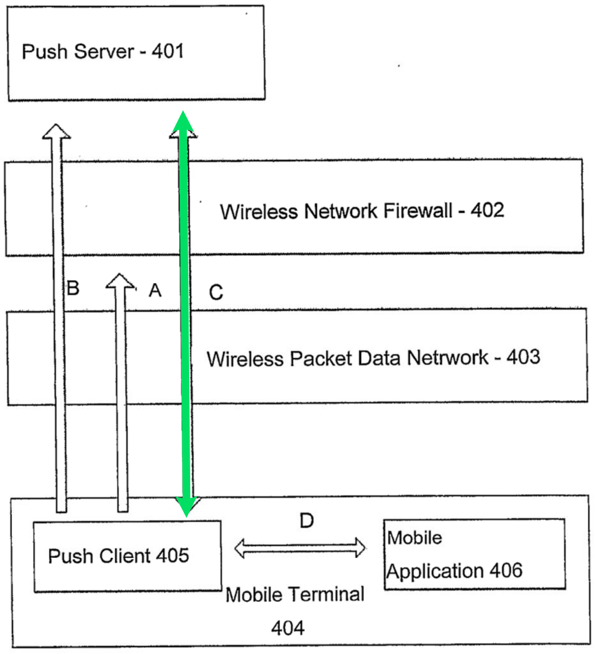
(a) Claim 22

Claim 22 requires that claim 1's "service control link" (Houghton-Ogawa's data connection C) "support[] periodic transmissions" by "the service control server link element" (Houghton-Ogawa's push server). EX-1003, ¶383.

Houghton expressly discloses "use of" "***periodic***" messages sent "***from***" the "***server to the client***" to ensure its connections are not "***time expired***." EX-1006*,* 19. These are "periodic transmissions," as claimed. EX-1003, ¶383.

Also, Houghton's push client "***may send a periodic message (the arrow C in Figure 4) from the client 405 to the server 401 to the effect that [the connection does] not time expire***." EX-1006, 26; *see also id.* 11 (disclosing "suitable keep alive message"). "***The client 405 may then wait for a reply or acknowledgement from the server 401***, and if the acknowledgement is received" (step 622), the client 405 waits for the next "connection refresh and test." *Id.* A POSITA understood that push client-initiated "periodic" messages, and the push server's acknowledgement messages to client-initiated periodic messages are each a "***periodic transmission***" (as claimed). EX-1003, ¶384 (citing EX-1006, 11).

Thus, a POSITA understood data connection C "supports periodic transmissions" between Houghton-Ogawa's push server and push client. EX-1003, ¶384.



EX-1006, FIG. 4 (annotated)

(b) Claim 26

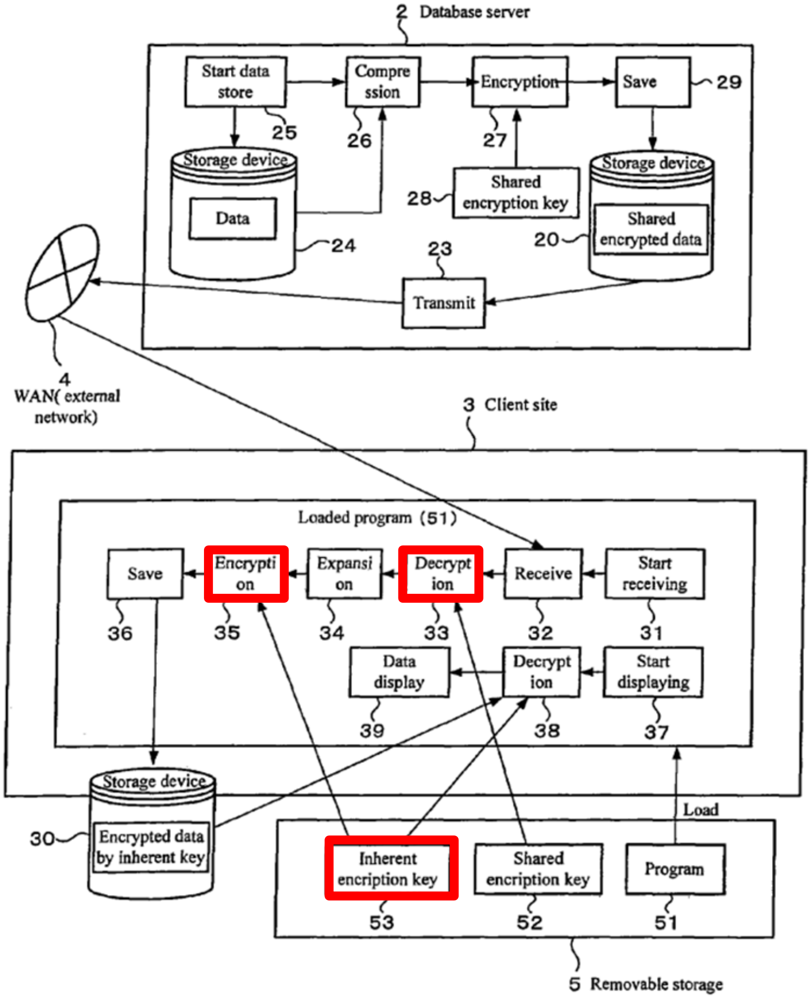
Claim 26 requires the "particular device agent" to "comprise[] software." A POSITA understood a mobile application to include software, and thus, understood that Houghton-Ogawa's mobile application ("particular device agent") "comprises software." EX-1003, ¶¶385-386 (citing EX-1006, 9, 16; EX-1016, 1:24-32; EX-1017, 1:54-2:5).

(c) Claim 27

Claim 27 calls the encryption key recited in claim 1 "a first encryption key," and requires claim 1's "service control device link agent" to be "configured to encrypt the message content using a ***second*** encryption key before delivering the message content to the particular agent." EX-1003, ¶387.

As discussed for claim 1, Houghton's push client is responsible for receiving a message from Houghton's push server, decrypting the message using a first encryption key, and sending message content to a destination application. EX-1003, ¶388.

As discussed *supra* §III.A.3(c), Ogawa discloses an encryption unit for re-encrypting data for, *e.g.,* transmission within the user device. EX-1005, 5:59-6:9; EX-1003, ¶389. Ogawa's inherent encryption key 53 is a second encryption key that is different from the first encryption key and is used to encrypt/decrypt data transmitted within the user device. EX-1003, ¶389 (citing EX-1005, 5:59-6:9, 5:24-25).



EX-1005, FIG.7 (annotated)

As discussed *supra* §III.A.3(c), a POSITA had reason to include the encryption functionality as part of Houghton's push client—*e.g.,* to secure decrypted received data before transmitting it to any other component on the user device. EX-1003, ¶390.

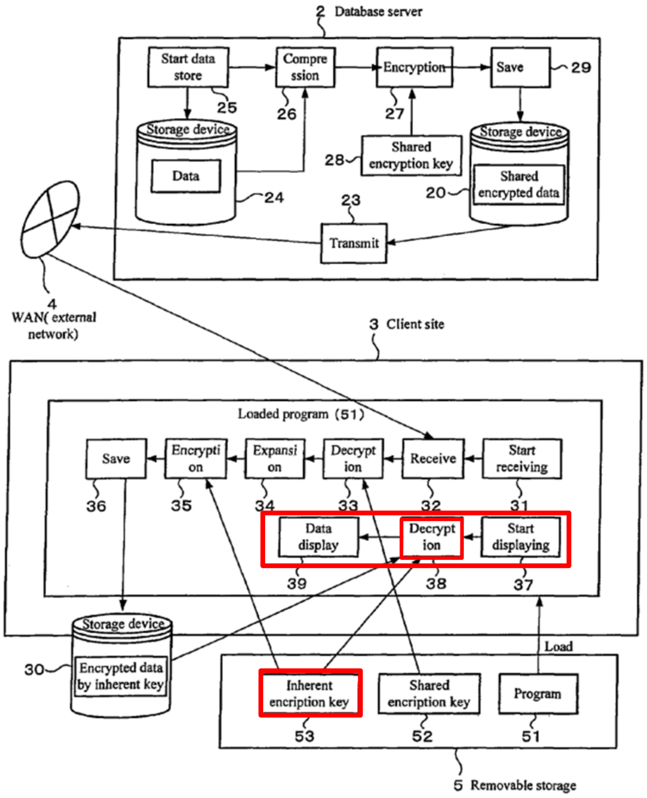
A POSITA would further have been motivated to implement Houghton-Ogawa's push client to secure/encrypt received message content using a different encryption key than the one used to decrypt the received data prior to delivery to device storage or the destination application, as taught by Ogawa. EX-1003, ¶391; EX-1005, 6:1-26. Such internal encryption taught by Ogawa would have improved data security in Houghton-Ogawa's user device when stored on the device or when transmitted within the terminal, and would have helped, *e.g.*, prevent unauthorized viewing or use of the data by rogue/unauthorized device software. EX-1003, ¶391.

A POSITA would also have had reason to implement Houghton-Ogawa's push client such that it performed any intermediary functions/steps between decryption (*e.g.*, by Ogawa's unit 33) and re-encryption (e.g., by Ogawa's unit 35) that were required to ensure that the destination (on the user device) received data with correct format and content. EX-1003, ¶392 (citing EX-1005, 5:65-6:3). A POSITA would have reasonably expected success implementing Houghton-Ogawa's push client to perform the intermediary functions described in Ogawa—*e.g.,* by incorporating expansion unit 34—because the prior art components would continue to perform functions they performed prior to the combination: the push client would continue to receive, decrypt, and send data to another component on the user device, and Ogawa's expansion and encryption units (implemented within the push client) would convert decrypted data into its original format before encrypting it for use within the user device. EX-1003, ¶392.

Claim 27 also requires "the second encryption key" to be "shared by the service control link agent and the particular agent." EX-1003, ¶393.

As noted for claim 19, Houghton-Ogawa's user device is capable of displaying messages to a user. EX-1003, ¶394. As discussed below, a POSITA had reason to implement Houghton-Ogawa's user device such that it could display data encrypted using Ogawa's inherent key 53 (discussed above).

Ogawa teaches using "display units 37-39" to "render[] decoded data to a display of" the client. EX-1005, 5:24-30, 6:10-18. To "render" and display data stored on the client, decryption unit 38 decrypts the data using the same inherent key 53 that was used to encrypt the data for storage within the device. *Id.*; EX-1003, ¶394.



EX-1005, FIG. 7 (annotated)

Based on Ogawa's teachings, a POSITA had reason to incorporate Ogawa's display units 37-39 into Houghton-Ogawa's user device to be able to decrypt and display data decrypted using Ogawa's inherent key 53. EX-1003, ¶395. A POSITA would have reasonably expected success doing so, because the prior art components would continue to perform functions they performed prior to the combination. *Id.*

In such an implementation, for data received by the push client from the push server that was intended for immediate display to the user, a POSITA understood that Houghton-Ogawa's display units 37-39 collectively constituted a destination application that performed display functions on behalf of an entity (*e.g.*, client, server, another application), thus constituting one of the "***plurality of device agents***" for [1b], and "***a particular device agent***" for [1d3], in claim 1. EX-1003, ¶396.

Because both the push client and Houghton-Ogawa's display units 37-39 use the same key for encryption and decryption, a POSITA understood that the inherent key (***second encryption key***) is ***shared*** by encryption unit 35 in the push client (***the service control device link agent***) and the destination display units 37-39 (***the particular agent***). EX-1003, ¶397.

(d) Claim 28

Claim 28 requires claim 1's "service control device link agent" to be "configured to trigger a device transmission to maintain the service control link when a time between transmissions would otherwise cause the service control link to terminate." EX-1003, ¶398.

The '733 Patent discloses a "transmission trigger" "that triggers a transmission according to… ***a maximum time between transmissions clock*** to keep the service processor 115 in communication with the service controller 122 ***when little or no service usage is occurring***…." EX-1001, 38:19-25. Similarly, Houghton's push client 405 periodically pings push server 401 with "***a suitable keep alive message***" to keep data connection C (the "***service control link***") between the client and the server alive. EX-1006, 11, 26; *see also*, EX-1006, 27, 19. A POSITA understood that if such pings are not sent before the connection time expired, data connection C would terminate. EX-1003, ¶398.

(e) Claim 29

Claim 29 requires claim 1's "service control link" which "is configured to support control-plane communications" to be configured for such communications "using an Internet protocol." As discussed for [1a1]-[1a2], data connection C (the "***service control link***") supports control-plane communications. Houghton characterizes data connection C as being implemented using a "connection-oriented protocol such as TCP/IP, HTTP, or HTTPS." EX-1006, 20. A POSITA thus understood that Houghton-Ogawa's data connection C used an Internet Protocol because these were well-known secure Internet protocols. EX-1003, ¶399. Alternatively, this would have been a conventional, obvious way to implement what Houghton describes, and involves utilizing familiar, known components to achieve a predictable, desirable result of enabling Houghton's mobile terminal to send and receive data over the Internet. *Id*. Thus, Houghton-Ogawa's data connection C (the "***service control link***") "is configured to support control-plane communications using an Internet Protocol." *Id.*

B. Ground 3: Claims 3, 4, 6, 11, 12, 16-18, 23, 24 Are Obvious Over Houghton-Ogawa and Hwang

1. Hwang

Hwang describes establishing a roaming connection between a mobile device and a visited server when the terminal enters the server's roaming area. EX-1007, [1], [35]; EX-1003, ¶¶400-401.

FIG. 8 (below) illustrates a communication sequence between a mobile terminal 800 and a Visited Service Provider (Visited SP) 810 when the terminal "arrives at" Visited SP 810's "roaming area." EX-1007, [97], [100]. To establish a roaming connection with Visited SP 810, mobile terminal 800 sends a request (803) to Visited SP 810 for roaming registration. EX-1007, [102-104]. Visited SP 810 sends (806) a response including Roaming Service Allowed Scope that indicates the scope and charge of the roaming service. *Id.*, [110-112]. If terminal 800 communicates (807) to the Visited SP that it agrees with the Roaming Service Allowed Scope, Visited SP 810 starts providing roaming services (809) to the terminal. *Id.*, [113], [115].

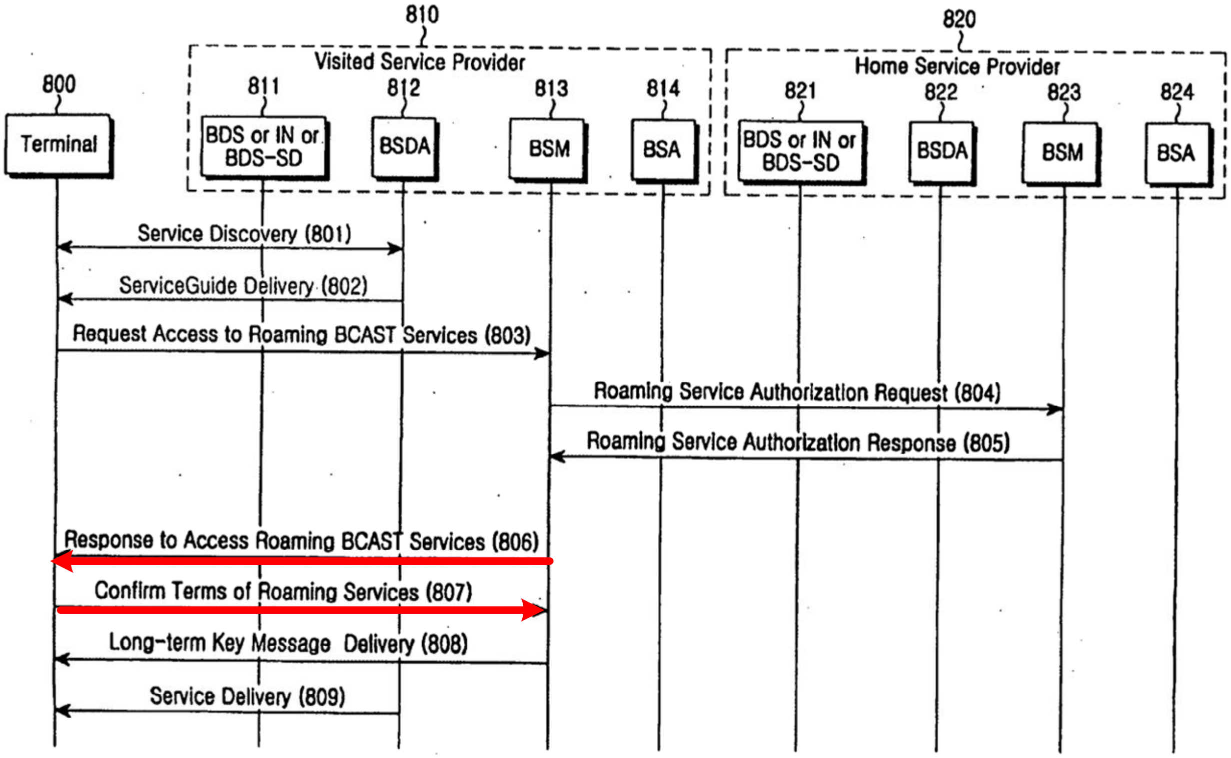

810
Visited Service Provider
820
Home Service Provider
800
Terminal
811
BDS or IN or BDS-SD
812
BSDA
813
BSM
814
BSA
821
BDS or IN or BDS-SD
822
BSDA
823
BSM
824
BSA
Service Discovery (801)
ServiceGuide Delivery (802)
Request Access to Roaming BCAST Services (803)
Roaming Service Authorization Request (804)
Roaming Service Authorization Response (805)
Response to Access Roaming BCAST Services (806)
Confirm Terms of Roaming Services (807)
Long-term Key Message Delivery (808)
Service Delivery (809)

FIG.8

EX-1007, FIG. 8 (annotated)

2. Houghton-Ogawa and Hwang Combination

A POSITA would have found it obvious to combine Houghton's and Hwang's teachings, and would have been motivated to do so, for the reasons described below. EX-1003, ¶¶402-408.

First, a POSITA would have been motivated to apply Hwang's roaming initiation technique to Houghton's push messaging system to enable the end-user to receive and benefit from network services even while the end-user is away from his/her home network. EX-1003, ¶¶403-404. Houghton recognizes the need for delivering "real time information, interactivity and rich media content, ***regardless of*** which mobile operator is being used and ***where the mobile user happens to be***

at that moment." EX-1006, 10-11. Houghton, however, does not explicitly disclose how to establish a roaming service for a mobile terminal that exits the user's home network. EX-1003, ¶403. A POSITA would thus have turned to roaming-related references, like Hwang, for implementation details. EX-1003, ¶403; *see also* EX-1007, [35]. Hwang discloses a communication sequence between a user's mobile terminal—Hwang's terminal 800—and a visited service provider (VSP) 810 before VSP 810 starts providing roaming services to the user device. EX-1007, ¶¶[110-113]; *see supra* §III.B.2 (describing this communication sequence); EX-1003, ¶404.

Second, a POSITA understood that implementing Hwang's roaming initiation techniques within Houghton-Ogawa's system would have beneficially ensured that the user of Houghton-Ogawa's mobile terminal and push server agreed to the terms and billing policies of a visited network before the push server started providing services (*e.g.*, by sending messages) to the mobile terminal. EX-1003, ¶405.

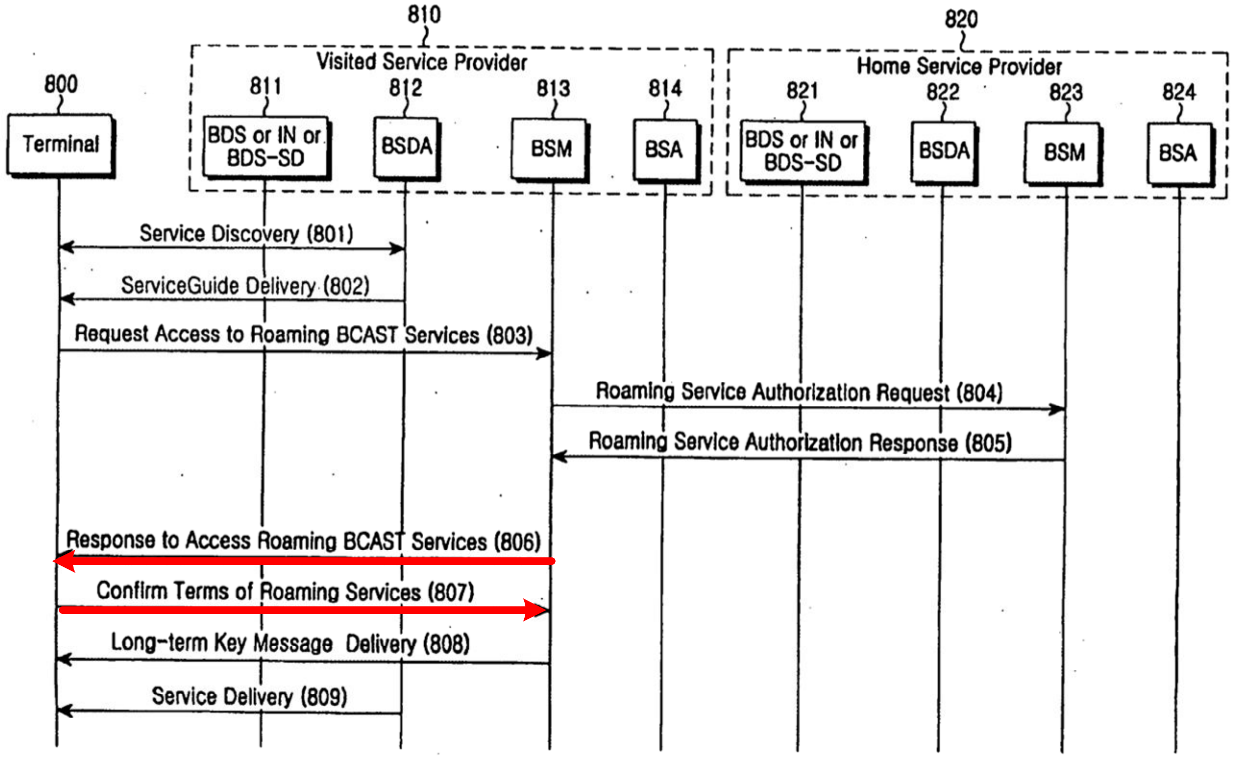

810
Visited Service Provider
820
Home Service Provider
800
Terminal
811
BDS or IN or BDS-SD
812
BSDA
813
BSM
814
BSA
821
BDS or IN or BDS-SD
822
BSDA
823
BSM
824
BSA
Service Discovery (801)
ServiceGuide Delivery (802)
Request Access to Roaming BCAST Services (803)
Roaming Service Authorization Request (804)
Roaming Service Authorization Response (805)
Response to Access Roaming BCAST Services (806)
Confirm Terms of Roaming Services (807)
Long-term Key Message Delivery (808)
Service Delivery (809)

FIG.8

EX-1007, FIG. 8 (annotated)

Third, implementing these techniques in the form described in Hwang and within the service-providing environment disclosed in Houghton would have been nothing more than implementing a known method within known systems to achieve predictable results. EX-1003, ¶406.

A POSITA would have reasonably expected success applying Hwang's roaming initiation technique to Houghton-Ogawa because Houghton provides the required infrastructure (a server that provides roaming services, and a mobile terminal device that uses the roaming services), and Hwang provides a technique to establish an agreement between the visited service provider (*e.g.*, implemented within Houghton-Ogawa's push server) and a roaming mobile terminal, before any roaming services commence. EX-1003, ¶407.

Moreover, in the combination, Hwang's roaming authorization and messaging functionality would readily achieve Hwang's goals (*i.e.*, establishing a roaming connection) while enabling roaming services for Houghton—thus ensuring a reasonable expectation of success in the resulting combination. EX-1003, ¶408 (citing EX-1006, 18; EX-1007, ¶¶[0100-0102]). The resulting combination—in which Houghton-Ogawa's push server is implemented to incorporate Hwang's roaming authorization and messaging functionality of Visited SP 810 as described above—is referred to herein as Houghton-Ogawa-Hwang.

3. Claim Analysis

(a) Claims 3-4

Claim 3 requires claim 1's "message content" to "comprise[] information associated with a service usage." Claim 4 requires the "information" to be "about" "a service usage value," "a projected service usage value," or "a service usage plan limit." EX-1003, ¶409.

The '733 Patent indicates that "service usage" can include usage of "roaming" services by the end-user device and lists roaming costs as an example of service usage. EX-1003, ¶410 (citing EX-1001, 58:1-14, 53:7-10).

Hwang discloses sending messages containing information about roaming service usage to end-user devices. EX-1003, ¶411. A POSITA understood that the "Roaming Service Allowed Scope" sent as part of Hwang's message 806 is "associated with a ***service usage***," as recited in claim 3, because it includes the "reception rights" and charging policies to be applied to Houghton-Ogawa's mobile terminal for use of roaming services that Visited SP 810 provides. EX-1007, ¶¶[0112], [0108].

Information about charging policies disclosed in Hwang also include "additional costs" associated with receiving the roaming services (which a POSITA understood constituted "***a service usage value***," as recited in claim 4), and "a change in the charging system" (which a POSITA understood constituted "***a <u>projected</u> service usage value***"). *Id.*; *see also id.*, ¶[0121]; EX-1003, ¶411. A POSITA also understood that Hwang's "reception rights" constituted the claimed "***service usage plan limit***" because they indicate "which reception right the roaming Terminal 800 will have in the Visited SP 810," for example "a class of the service that the roaming-requested Terminal 800 can receive from the roaming-requested Visited SP 810." *Id.*; EX-1003, ¶412.

The information included in Hwang's message 806 is similar to the roaming information that the '733 patent says is sent from a roaming server, which does not require the information to be sent to a particular application, or otherwise be application-specific. EX-1003, ¶413 (citing EX-1001, 61:15-31). Rather, information regarding the roaming service usage in the '733 Patent is directed to the device, as a whole, using the roaming service. Accordingly, a POSITA understood that Houghton-Ogawa-Hwang's message content (pushed from VSP 810 to the mobile terminal) comprises information that meets claims 3 and 4. EX-1003, ¶413.

(b) Claims 6, 11, 12

Claim 6 requires claim 1's "message content" to "comprise[] information associated with a roaming service usage or a roaming service cost." Claim 11 requires the "message content" to "comprise[] information associated with a service policy." Claim 12 requires it to "comprise[]service usage accounting information."

As discussed for claims 3-4, a POSITA understood that Houghton-Ogawa-Hwang includes message content (of message 806) comprising information associated with claim 6's "***roaming service usage***," because Hwang's "reception rights" information pertains to a mobile terminal using the roaming service. This information is likewise associated with claim 6's "***roaming service cost***," because Hwang's message includes information related to additional costs and changes in the charging system from using the roaming service. The information is likewise associated with claim 11's "***service usage accounting information***," because

Hwang's message includes information regarding the change in the charging system due to using the roaming service, which a POSITA understood pertains to how service usage is quantified for charging purposes. EX-1003, ¶¶414-415.

Houghton-Ogawa-Hwang also includes message content that comprises information associated with "***a service policy***" (*e.g.*, reception rights or charging policies associated with the roaming services). VSP 810 sends (806) a message to the mobile terminal to inform the terminal's user about the service terms (*e.g.*, charging policies) for the roaming service. EX-1003, ¶416 (citing EX-1007, ¶[0113]). A POSITA understood that this message includes details regarding policies for the roaming service, so that the user may accept or decline them in a response message (807). EX-1003, ¶416.

(c) Claims 16-18

Claims 16-18 depend from claim 15. Claim 16 requires claim 15's "user response" to "comprise[] an acknowledgment of a roaming cost or a roaming usage." Claim 17 requires "an acknowledgment of a service usage," or "a service cost." Claim 18 requires "an indication that a user intends to purchase a service plan."

Hwang says VSP 810 sends (806) a message to the mobile terminal to inform it about the service terms such as charging policies associated with the roaming service. EX-1007, ¶¶[110-112]. The terminal's response (807) includes a "Roaming Confirm Status" "used for indicating whether" the terminal's user agreed with the Roaming Service Allowed Scope's terms and "will roam to… Visited SP 810"—*i.e.,* a "user response" as required by claim 15. EX-1007, ¶¶[0113-114]; EX-1003, ¶¶417-418. Because message 807 includes a response indicating whether the user confirms (and thus acknowledges) terms of the Roaming Service Allowed Scope (which includes a service cost), a POSITA understood the user response to include an "***acknowledgement of a roaming coast or roaming usage***" (claim 16), and "***acknowledgment of a service usage"*** or ***"service cost***" (claim 17)—where the service is the roaming service. EX-1003, ¶418. Further, a user response agreeing to the Roaming Service Allowed Scope through message 807 meets claim 18's "***indication of an intention to purchase the service plan***," because the user confirms reception rights for the offered price. *Id.*

(d) Claims 23-24

Claim 23 requires the "service control device link agent" (Houghton-Ogawa's push client) to be "configured to send" or "receive" a "device credential" to "the network system during a service authorization sequence." EX-1003, ¶419. Per claim 24, the "device credential" can include a "device identifier."

Houghton-Ogawa's push server, when implemented to function as Hwang's VSP 810, is part of a "network system" (discussed *supra* for [1a] and §III.B.2), because it is a server performing one or more server functions in Houghton-Ogawa-Hwang's network. EX-1003, ¶419.

Hwang uses a Terminal ID for each mobile terminal to keep track of roaming terminals. EX-1003, ¶420. Roaming Request 803 sent from the mobile terminal to VSP 810 (as the push server 401 in Houghton) includes the Terminal ID. EX-1007, ¶¶[0102-0103].

A POSITA understood that the Terminal ID is used "***during a service authorization sequence***," because it is used to determine whether the terminal is authorized to receive roaming services. EX-1003, ¶421. The sequence includes the roaming request 803 received from the terminal, and subsequent communications between Visited SP 810 and Home SP 820, including message 805 that includes a terminal's Roaming Authorization Status, which is determined by retrieving the terminal's subscription, using the Terminal ID. *Id.*; EX-1007 ¶¶[0105-108]).

Because Houghton-Ogawa's push client 404 ("***service control device link agent***") exchanges communications with the push server, a POSITA understood, in Houghton-Ogawa-Hwang, that push client 404 is configured to send a "***device credential***" (claim 23)—Hwang's Terminal ID—to push server 401, which constitutes a "***device identifier***" (claim 24). EX-1003, ¶422.

IV. PTAB DISCRETION SHOULD NOT PRECLUDE INSTITUTION

A. §325(d)

The references advanced in this Petition were not previously before the Office. *See generally* EX-1002. Thus, the Office has not considered the references or combinations presented in this Petition. Moreover, the same or substantially the same arguments were not previously presented to the Office. Indeed, there could be no overlap between the arguments made before the Office because the Examiner issued no prior art rejections during prosecution. *Id.*

Further, material error occurred during prosecution because Examiner failed to consider systems of the above-presented grounds, and how they rendered obvious every claim feature of the Challenged Claims. Indeed, Petitioners have shown a reasonable likelihood that at least one of the Challenged Claims is unpatentable over the applied art on the current record. *Supra* §III.A-B; *see Tokyo Ohka Kogyo Co., Ltd. v. Fujifilm Elec. Materials U.S.A., Inc.*, PGR2022-00010, Paper 9, 8-9 (PTAB June 6, 2022). Therefore, §325(d) discretionary denial is not warranted.

B. §314(a)

The Petition's merits are compelling, which "alone demonstrates that the PTAB should not discretionarily deny institution under *Fintiv*." EX-1020, 4-5. Moreover, the *Fintiv* factors do not favor denial.

Factor 1 favors institution because Google is not a party in the EDTX litigation and no litigation party (Samsung, Headwater) has requested a litigation stay.

Factor 2 favors institution because Google is not a party in the EDTX litigation, and the Court's trial date for the litigation parties (Samsung, Headwater) is speculative and subject to change. The Board will likely issue its Final Written

Decision around June 2025, 5-6 months after the currently scheduled trial date (January 6, 2025). EX-1022, 1. However, as the PTAB has recognized, "scheduled trial dates are unreliable and often change." EX-1020, 8.

Factor 3 favors institution because Google is not a party in the EDTX litigation. Moreover, Petitioners diligently filed this Petition months ahead of the one-year time bar for Samsung, while the EDTX Litigation is in its early stages. Indeed, by the anticipated institution decision deadline in June/July 2024, the litigation will still be in early stages—fact and expert discovery will be ongoing and the *Markman* hearing will not have occurred. *Id.*

Factor 4 favors institution because Google is not a party in the EDTX litigation and Samsung stipulates to not pursue the IPR grounds in the EDTX litigation. EX-1023. Thus, "[i]nstituting trial here serves overall system efficiency and integrity goals by not duplicating efforts and by resolving materially different patentability issues." *Apple, Inc. v. SEVEN Networks, LLC*, IPR2020-00156, Paper 10, 19 (June 15, 2020); *Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24, 12 (June 16, 2020); *Google LLC v. Flypsi, Inc.*, IPR2023-00360, Paper 9, 36-39 (August 2, 2023).

Factor 5 favors institution because Google is not a party in the EDTX litigation, so the parties in the EDTX litigation are not the same.

Factor 6 favors institution because the merits of this Petition are compelling.

V. CONCLUSION AND FEES

The Challenged Claims are unpatentable. Please charge fees to Deposit Account 06-1050.

VI. MANDATORY NOTICES UNDER 37 C.F.R §42.8(a)(1)

A. Real Party-In-Interest Under 37 C.F.R. §42.8(b)(1)

Samsung Electronics Co., Ltd. ("Samsung") and Google LLC ("Google") are the petitioners and real parties-in-interest. Samsung Electronics America, Inc. is an additional real-party-in-interest.

B. Related Matters Under 37 C.F.R. §42.8(b)(2)

The '733 Patent is the subject of *Headwater Research LLC v. Samsung Electronics Co., Ltd. et al.*, 2:23-cv-00103, E.D. Tex., filed March 10, 2023. Samsung and Headwater are also involved in case nos. 2:22-cv-00422 and 2:22-cv-00467, also in E.D. Tex.

Petitioners are not aware of any other disclaimers, reexamination certificates, or IPR petitions addressing the '733 Patent.

C. Lead and Back-Up Counsel Under 37 C.F.R. §42.8(b)(3)

Petitioners provide the following designation of counsel.

Lead Counsel	Backup counsel
W. Karl Renner, Reg. No. 41,265 Fish & Richardson P.C. 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070	Jeremy J. Monaldo, Reg. No. 58,680 Karan Jhurani, Reg. No. 71,777 60 South Sixth Street, Suite 3200 Minneapolis, MN 55402 Tel: 202-783-5070

Fax: 877-769-7945 Email:IPR39843-0164IP2@fr.com	Fax: 877-769-7945 IPR39843-0164IP2@fr.com Gregory F. Corbett, pending admission *pro hac vice* Turhan F. Sarwar, pending admission *pro hac vice* Wolf, Greenfield & Sacks, P.C. 600 Atlantic Avenue Boston, MA 02210 Tel: 617-646-8000 Fax: 617-646-8646 Gregory.Corbett@wolfgreenfield.com TSarwar-PTAB@wolfgreenfield.com

D. Service Information

Please address all correspondence and service to the address listed above.

Petitioners consent to electronic service by email at IPR39843-0164IP2@fr.com Gregory.Corbett@wolfgreenfield.com, and TSarwar-PTAB@wolfgreenfield.com (referencing No. 39843-0164IP2).

Respectfully submitted,

Dated 01/23/2024

/Karan Jhurani/
W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Karan Jhurani, Reg. No. 71,777
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

(Control No. IPR2024-00342)

Attorneys for Petitioner Samsung

Gregory F. Corbett,
pending admission *pro hac vice*,
Turhan F. Sarwar,
pending admission *pro hac vice*,
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, MA 02210
T: 617-646-8000
F: 617-646-8646

Attorneys for Petitioner Google

CERTIFICATION UNDER 37 CFR §42.24

Under the provisions of 37 CFR §42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,998 words, which is less than the 14,000 allowed under 37 CFR §42.24.

Dated 01/23/2024

/Karan Jhurani/
W. Karl Renner, Reg. No. 41,265
Jeremy J. Monaldo, Reg. No. 58,680
Karan Jhurani, Reg. No. 71,777
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
T: 202-783-5070
F: 877-769-7945

Attorneys for Petitioner Samsung

Gregory F. Corbett,
pending admission *pro hac vice*,
Turhan F. Sarwar,
pending admission *pro hac vice*,
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, MA 02210
T: 617-646-8000
F: 617-646-8646

Attorneys for Petitioner Google

CERTIFICATE OF SERVICE

Pursuant to 37 CFR §§42.6(e)(4)(i) *et seq.* and 42.105(b), the undersigned certifies that on January 23, 2024, a complete and entire copy of this Petition for *Inter Partes* Review, Powers of Attorney, and all supporting exhibits were provided via Federal Express, to the Patent Owner, by serving the correspondence address of record as follows:

Headwater Research LLC
Outside Firm 1
110 North College Avenue, Suite 1116
Tyler, TX 75702

/Michael Stanwyck/
Michael Stanwyck
Fish & Richardson P.C.
60 South Sixth Street, Suite 3200
Minneapolis, MN 55402
(202) 626-7790